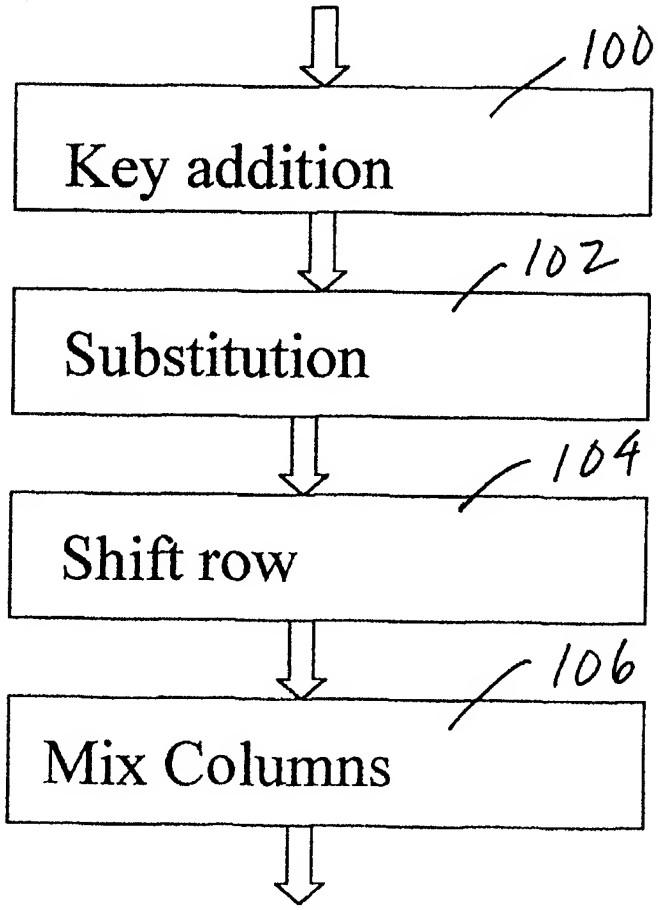


Fig. 1(a)

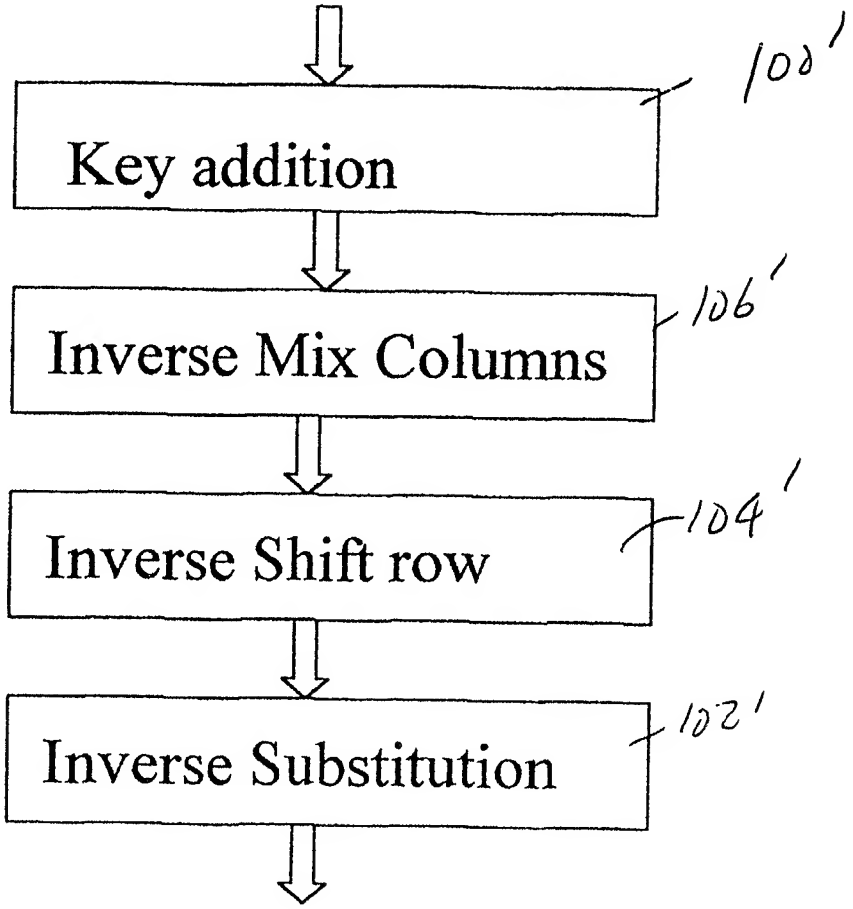


Figure 1(b)

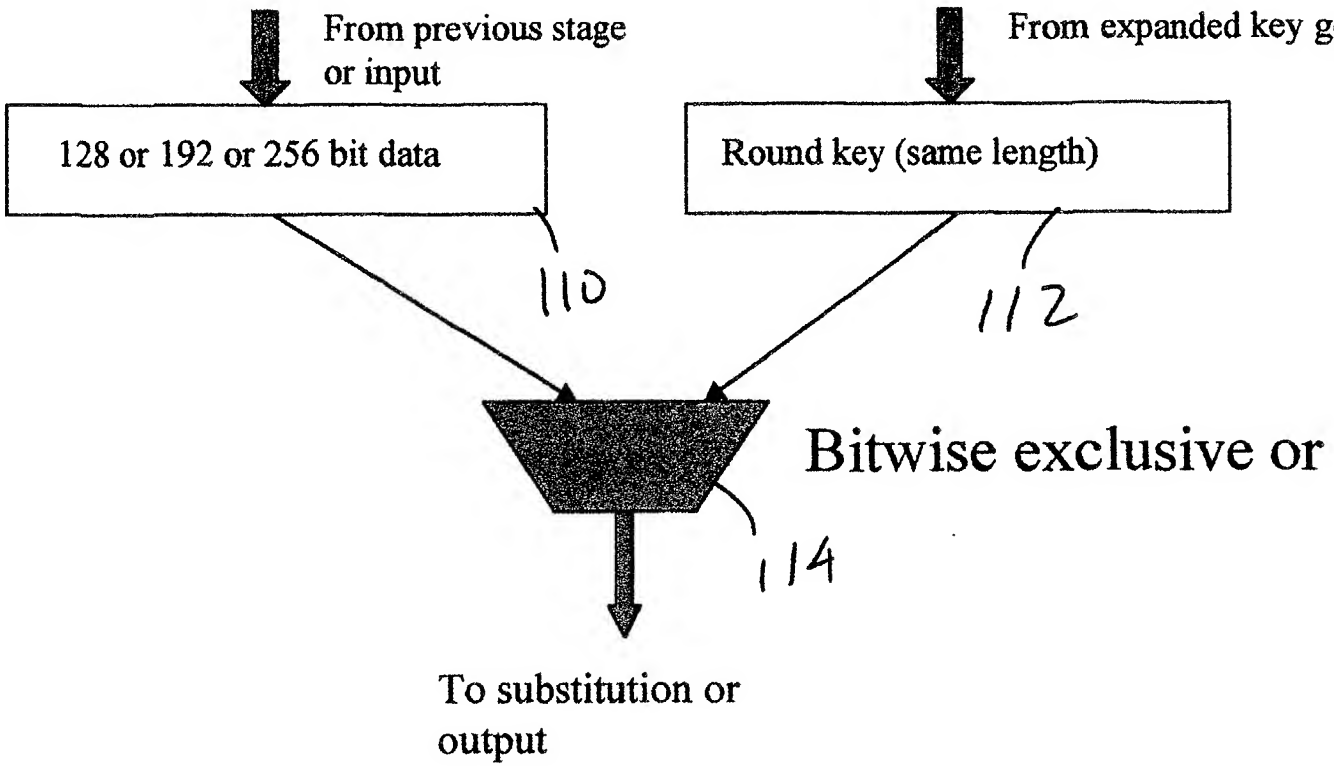

From previous stage or input
From expanded key generator
128 or 192 or 256 bit data
Round key (same length)
110
112
Bitwise exclusive or
114
To substitution or output

Fig. 2

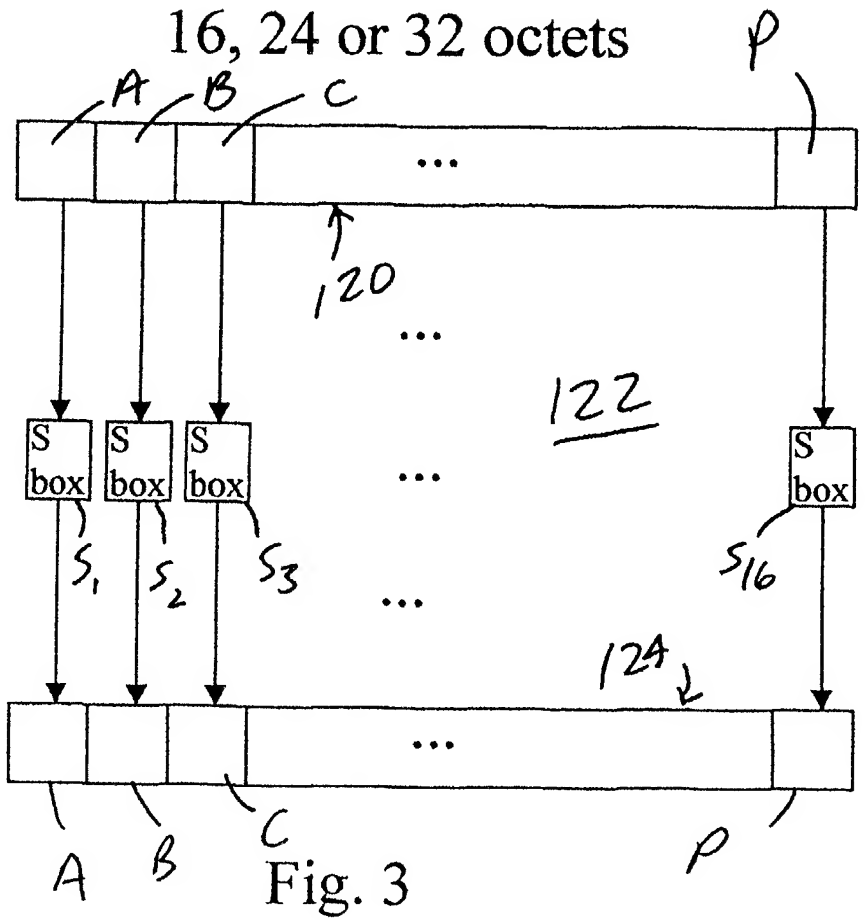

16, 24 or 32 octets
A
B
C
P
120
122
S box
S box
S box
S box
S1
S2
S3
S16
124
A
B
C
P

Fig. 3

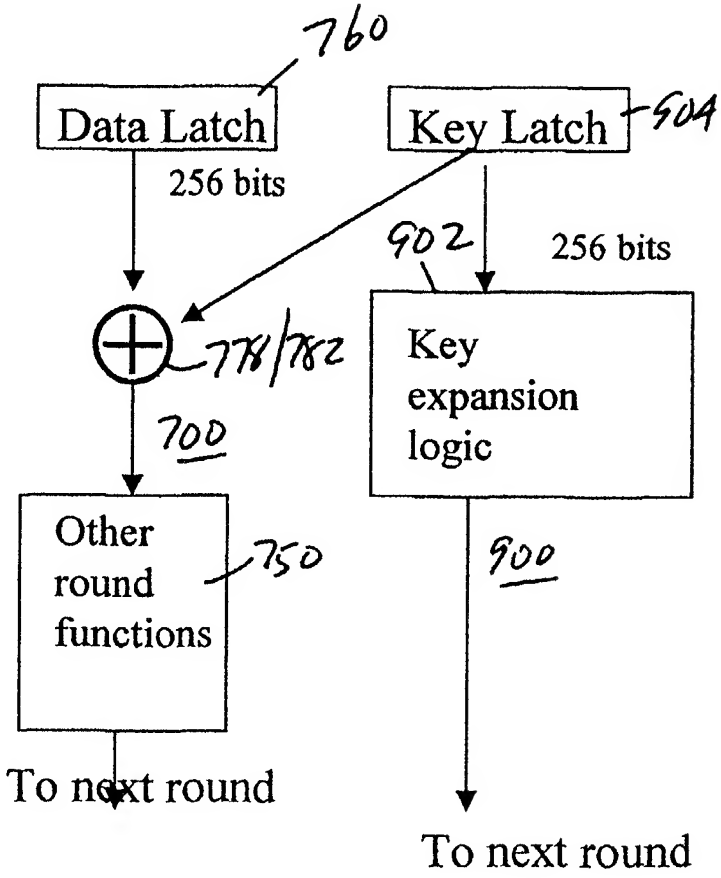

760
Data Latch
Key Latch
504
256 bits
902
256 bits
778/782
Key expansion logic
700
Other round functions
750
900
To next round
To next round

Fig. 39

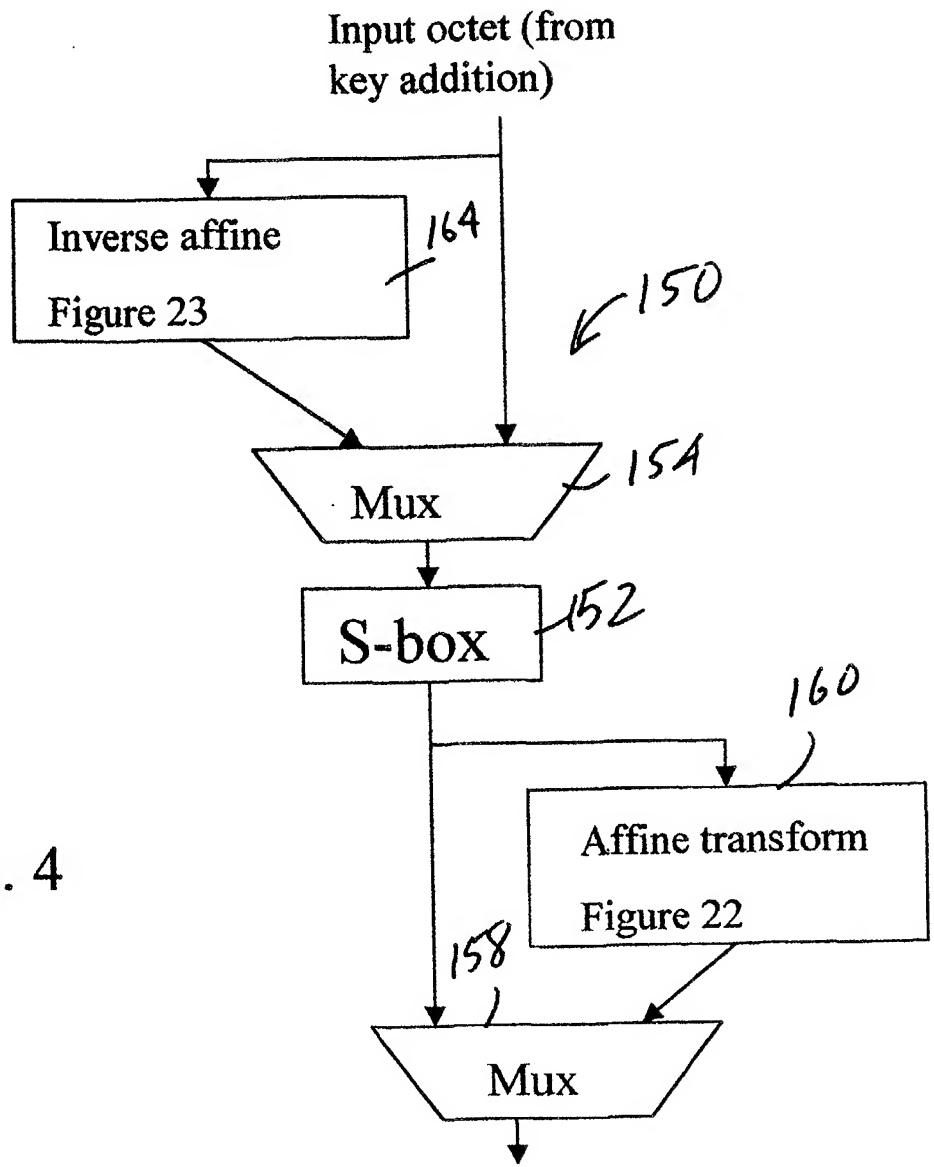

Input octet (from key addition)
Inverse affine
Figure 23
164
150
Mux
154
S-box
152
160
Affine transform
Figure 22
158
Mux

Fig. 4

Inverse Affine transform, decryption S-Box pre-processing

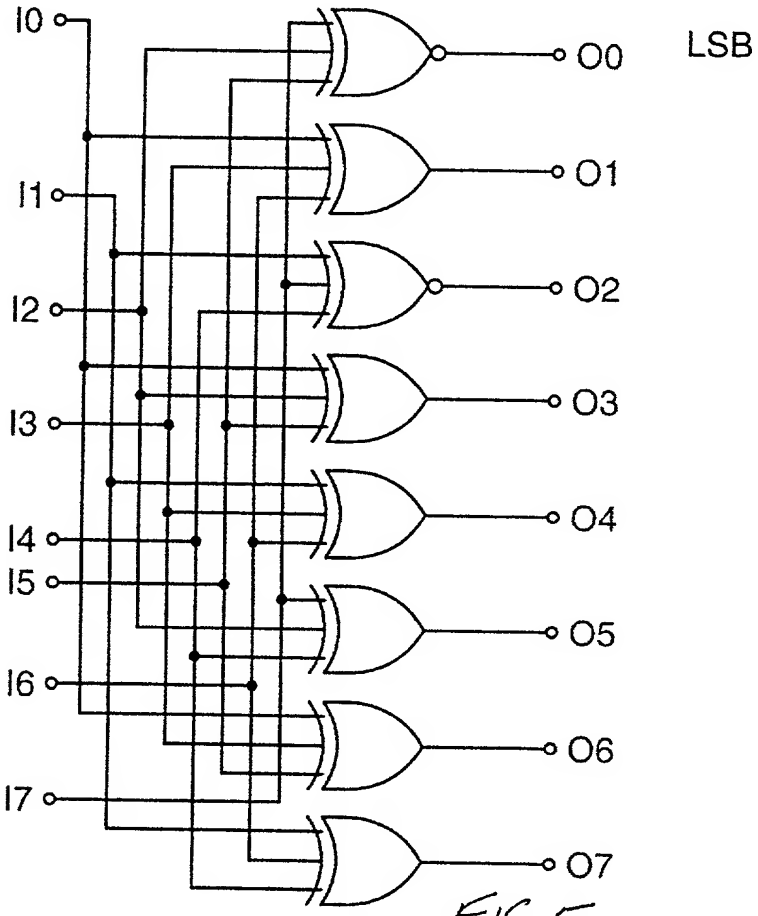


FIG. 5

Affine transform, encryption S-Box post processing

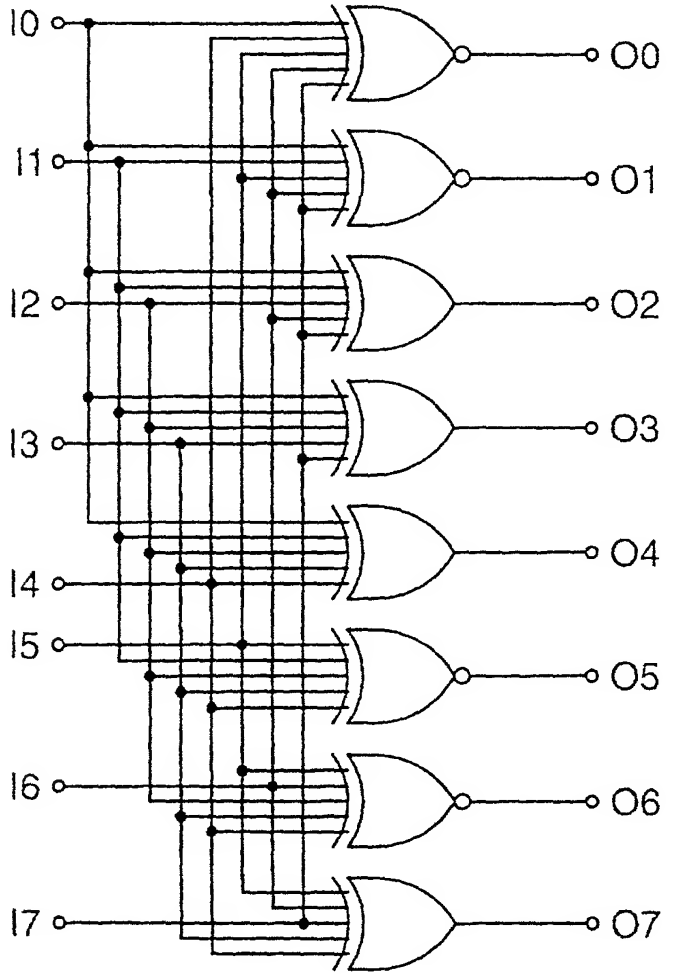


FIG. 6

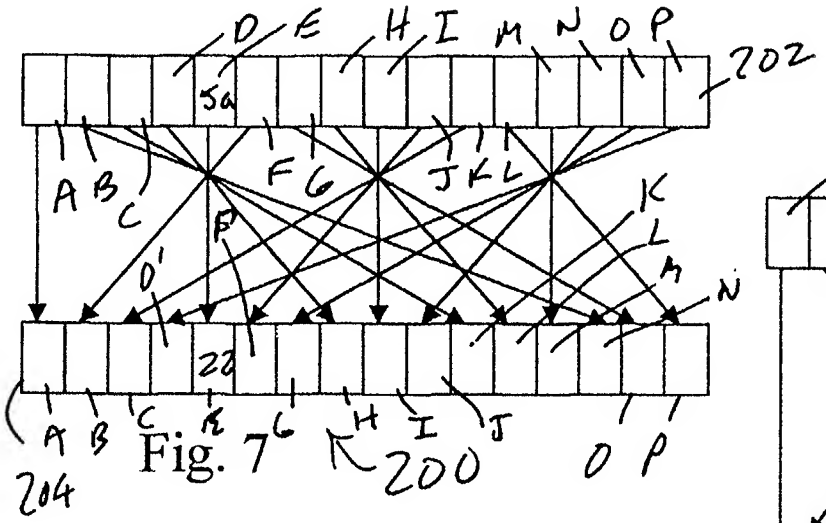


Fig. 7

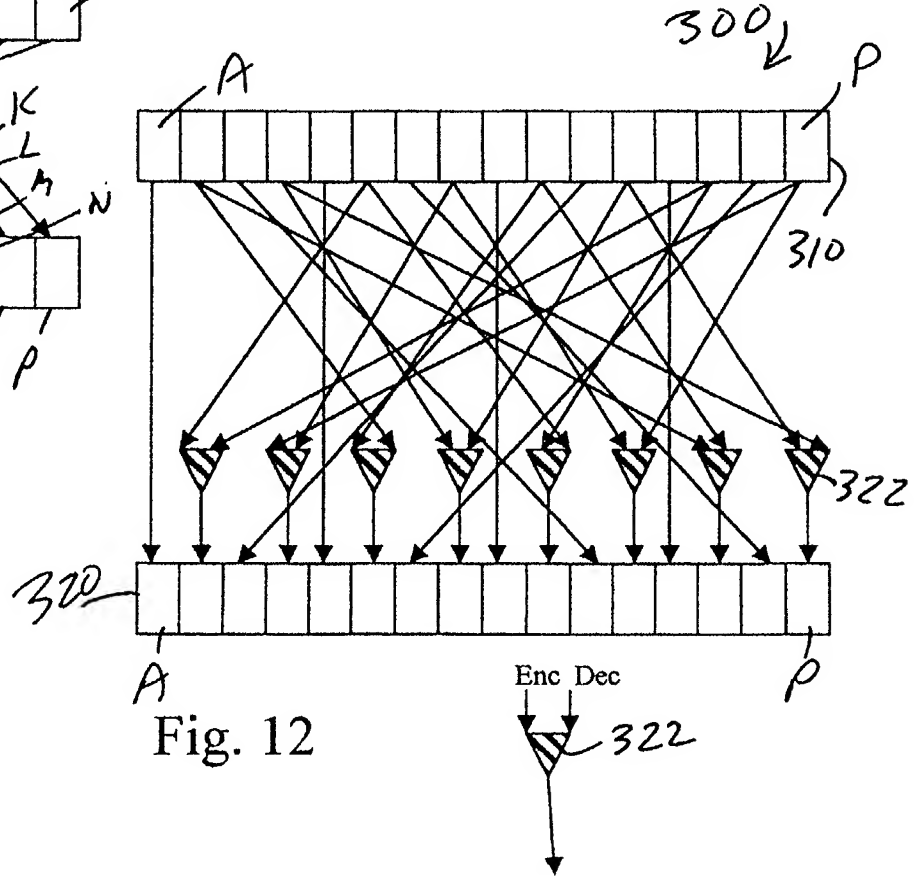


Fig. 12

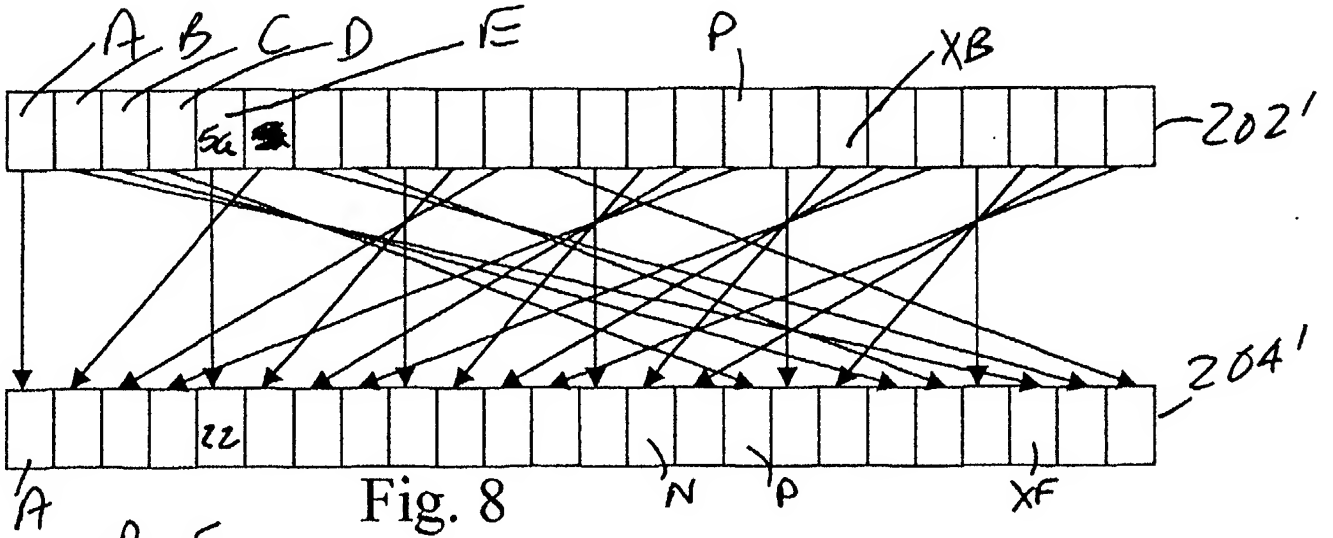


Fig. 8

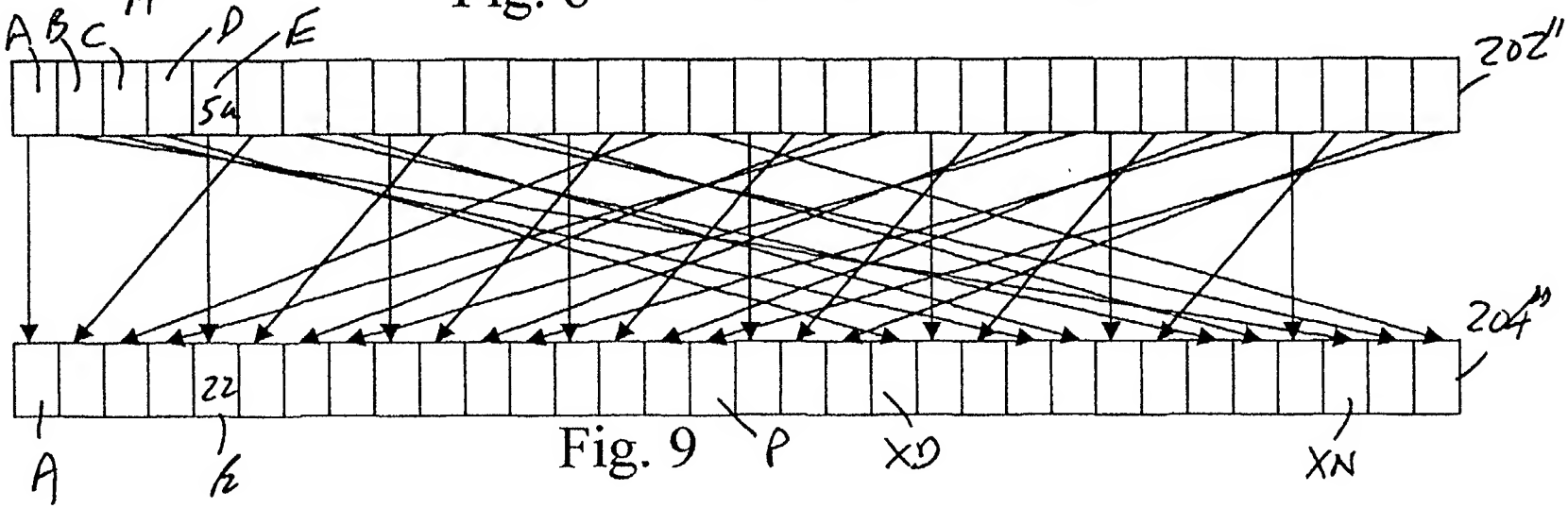


Fig. 9

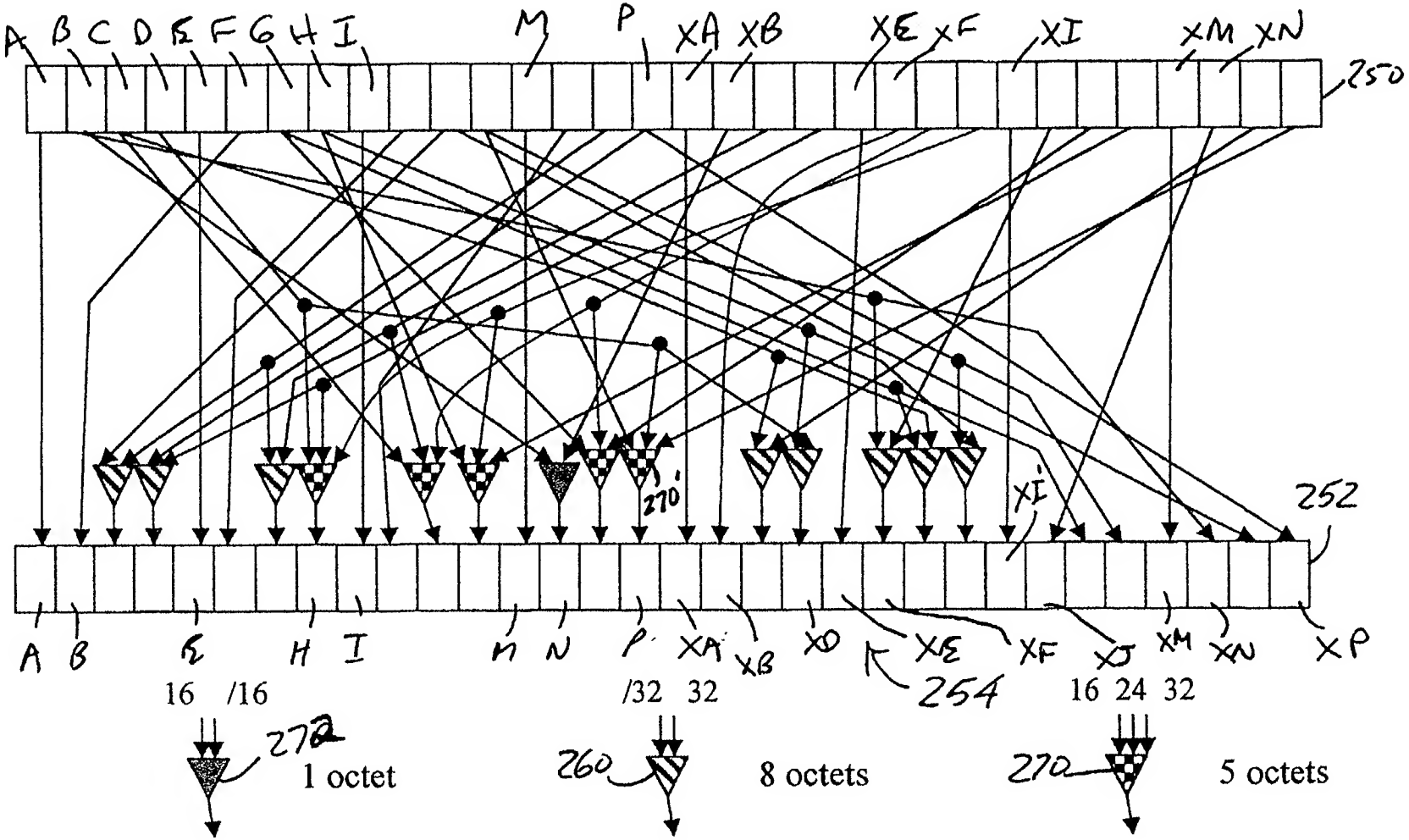

A B C D E F G H I M P XA XB XE XF XI XM XN
250
270'
XI'
252
A B E H I M N P XA XB XD XE XF XJ XM XN XP
16 /16
/32 32
16 24 32
254
272
1 octet
260
8 octets
270
5 octets

Fig. 10

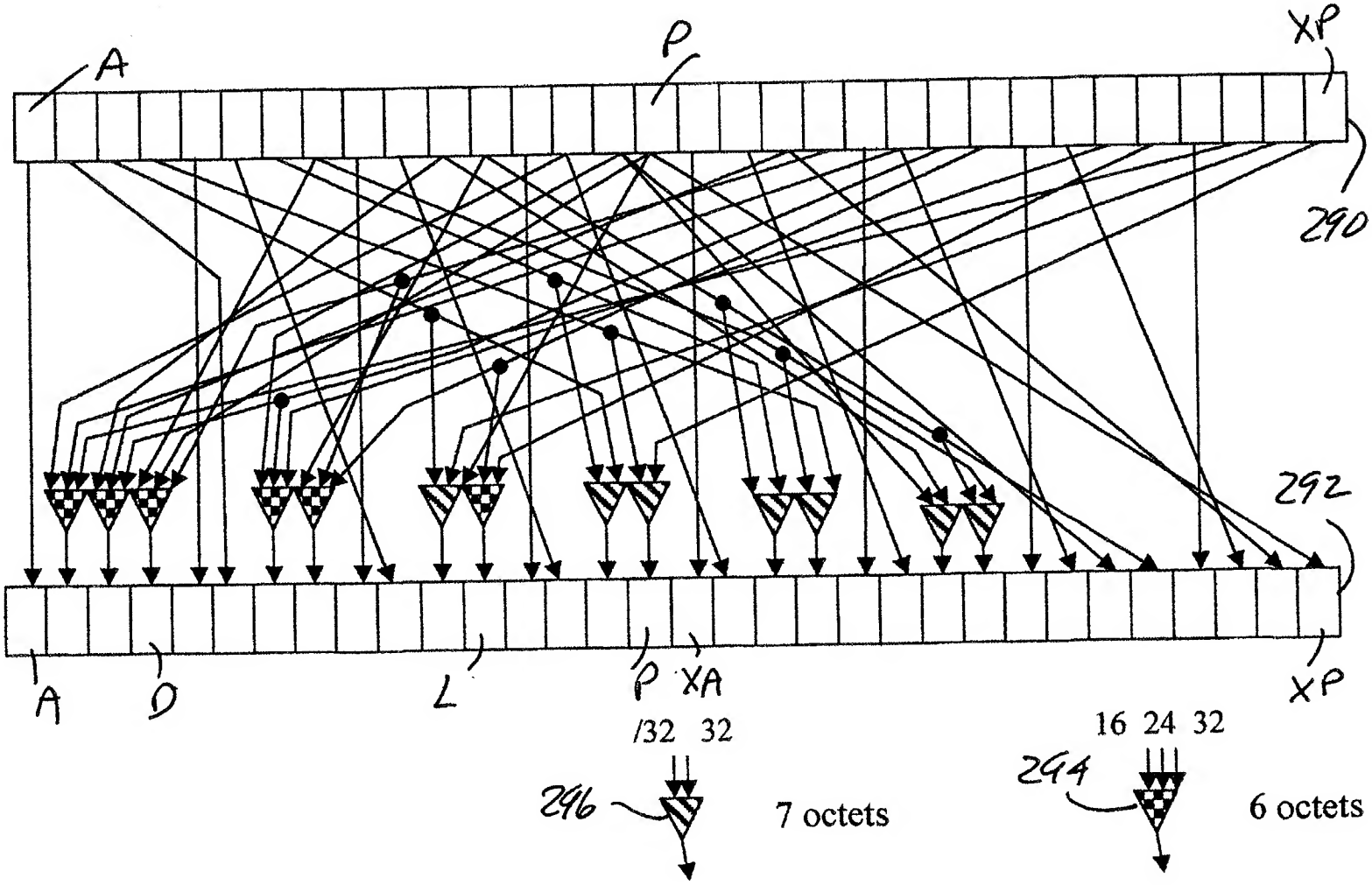


Fig. 11

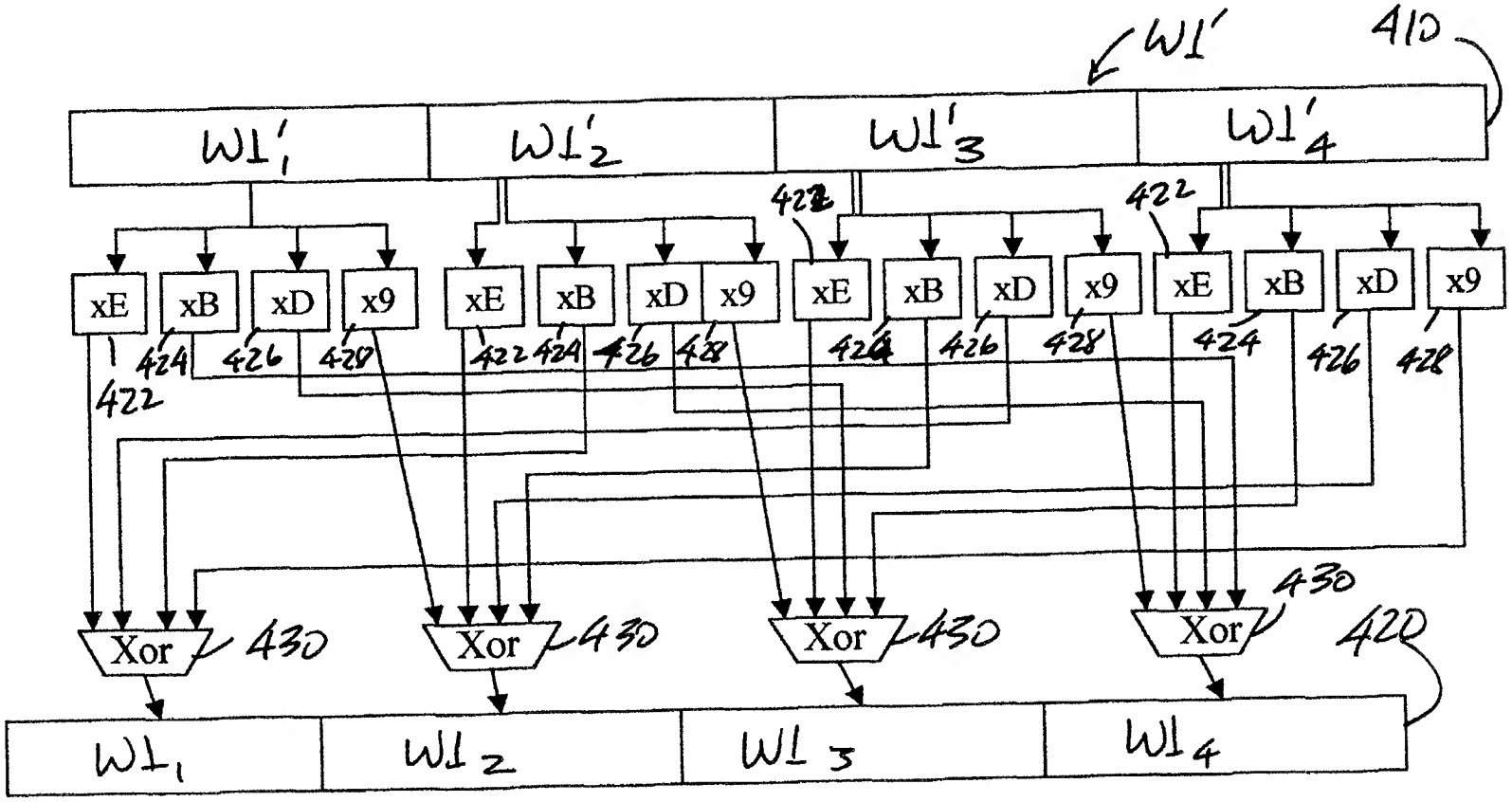

WL'
410
WL'1
WL'2
WL'3
WL'4
422
xE
xB
xD
x9
424
426
428
Xor
430
420
WL1
WL2
WL3
WL4
400

Fig. 14

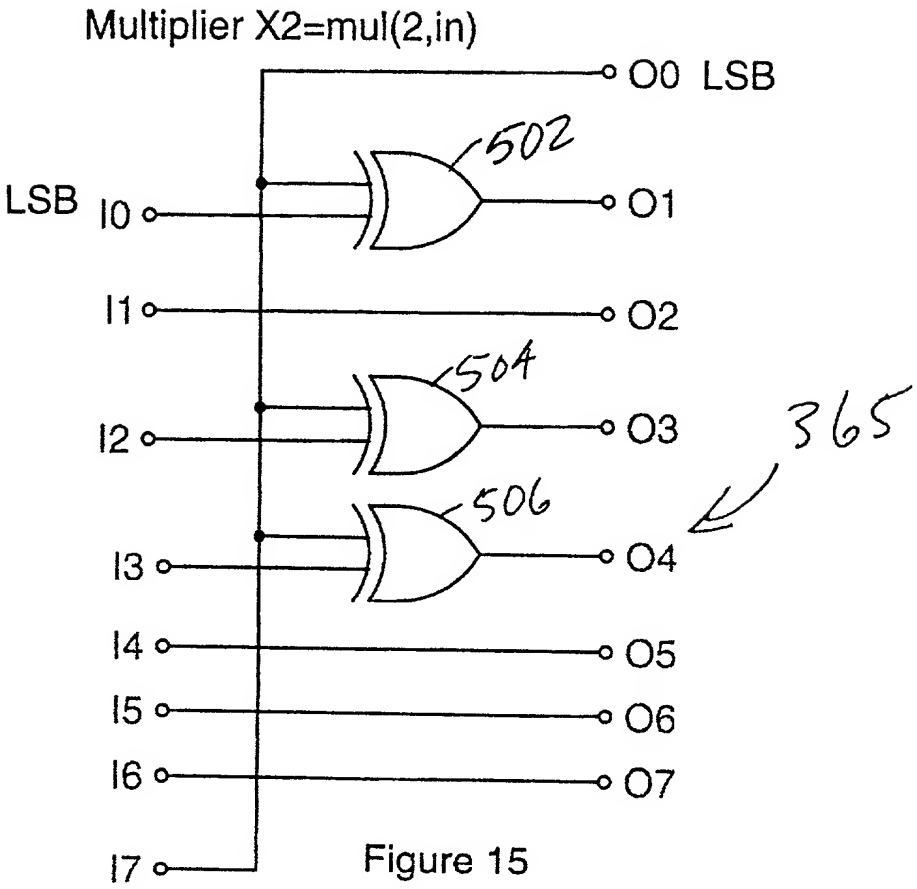

Multiplier X2=mul(2,in)
O0 LSB
502
LSB
I0
O1
I1
O2
504
I2
O3
365
506
I3
O4
I4
O5
I5
O6
I6
O7
I7

Figure 15

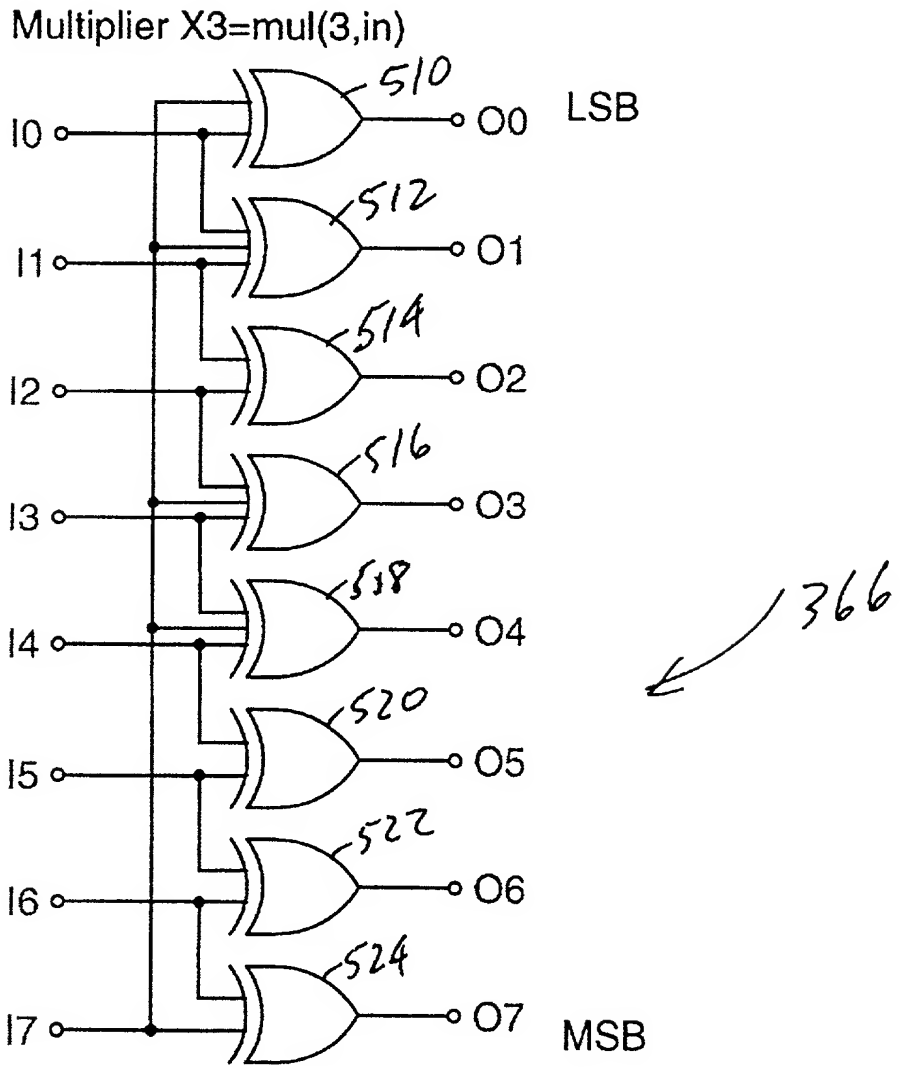

Multiplier X3=mul(3,in)
510
512
514
516
518
520
522
524
I0
I1
I2
I3
I4
I5
I6
I7
O0
O1
O2
O3
O4
O5
O6
O7
LSB
MSB
366

Figure 16

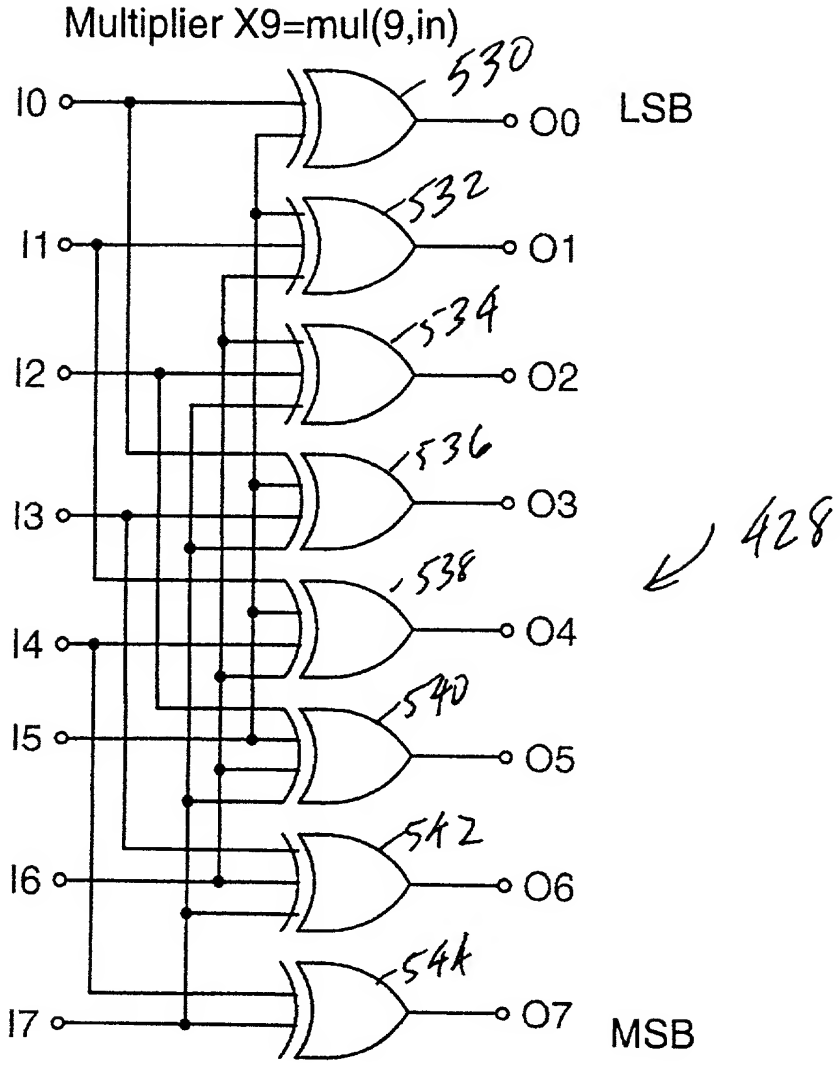

Multiplier X9=mul(9,in)
I0
I1
I2
I3
I4
I5
I6
I7
O0
O1
O2
O3
O4
O5
O6
O7
LSB
MSB
530
532
534
536
538
540
542
544
428

Figure 17

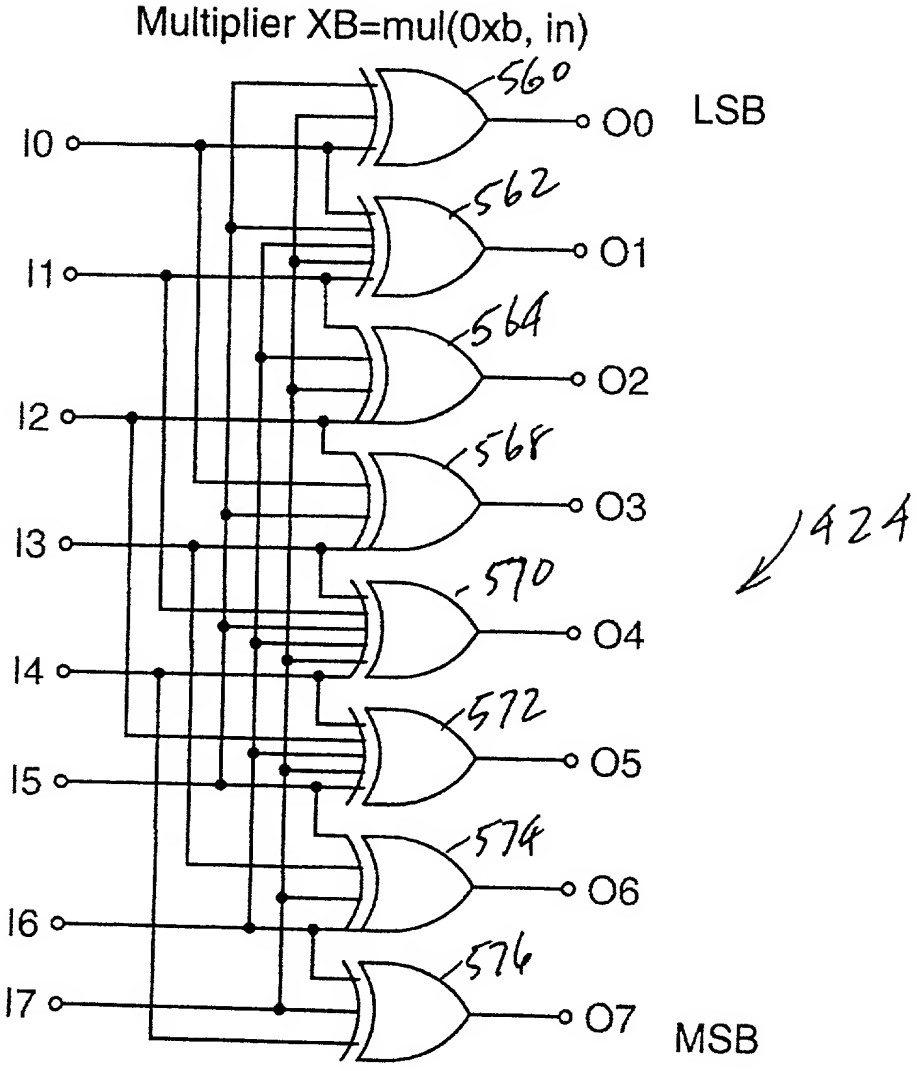

Multiplier XB=mul(0xb, in)
I0
I1
I2
I3
I4
I5
I6
I7
560
562
564
568
570
572
574
576
O0
O1
O2
O3
O4
O5
O6
O7
LSB
MSB
424

Figure 18

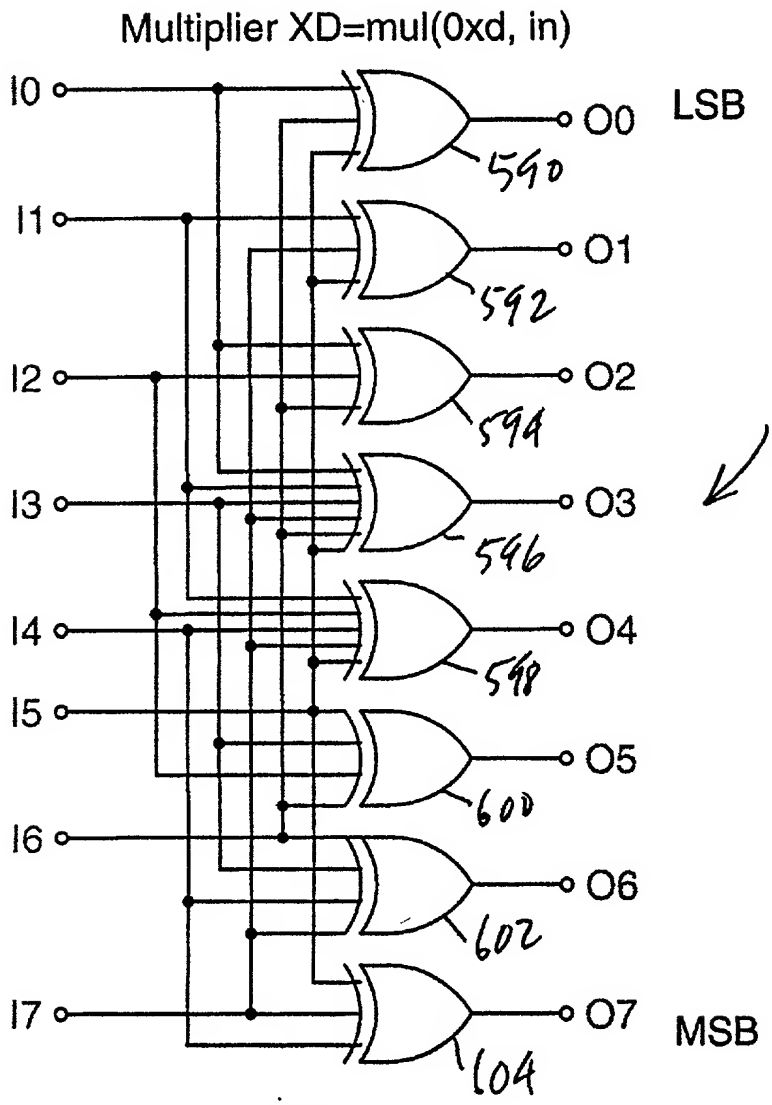

Multiplier XD=mul(0xd, in)
I0
I1
I2
I3
I4
I5
I6
I7
O0
O1
O2
O3
O4
O5
O6
O7
LSB
MSB
590
592
594
596
598
600
602
604
426

Figure 19

Multiplier XE=mul(0xe, in)

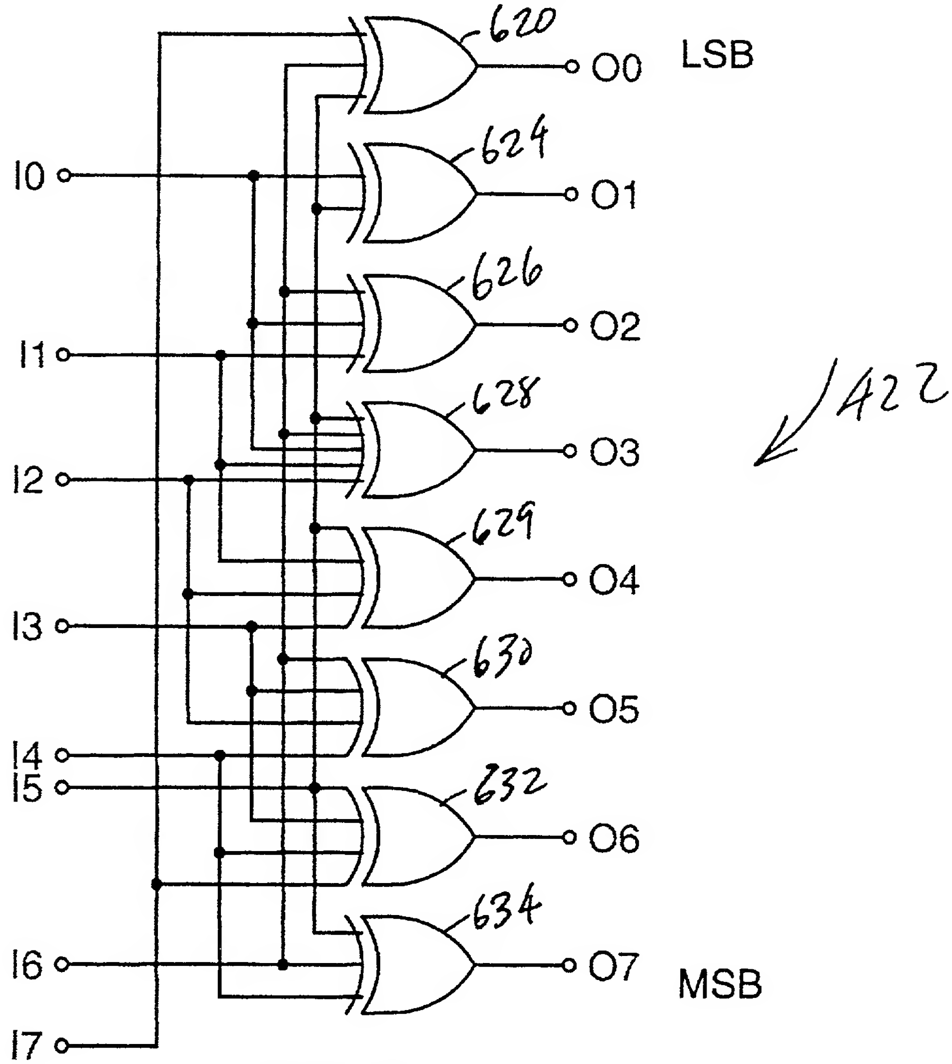


Figure 20

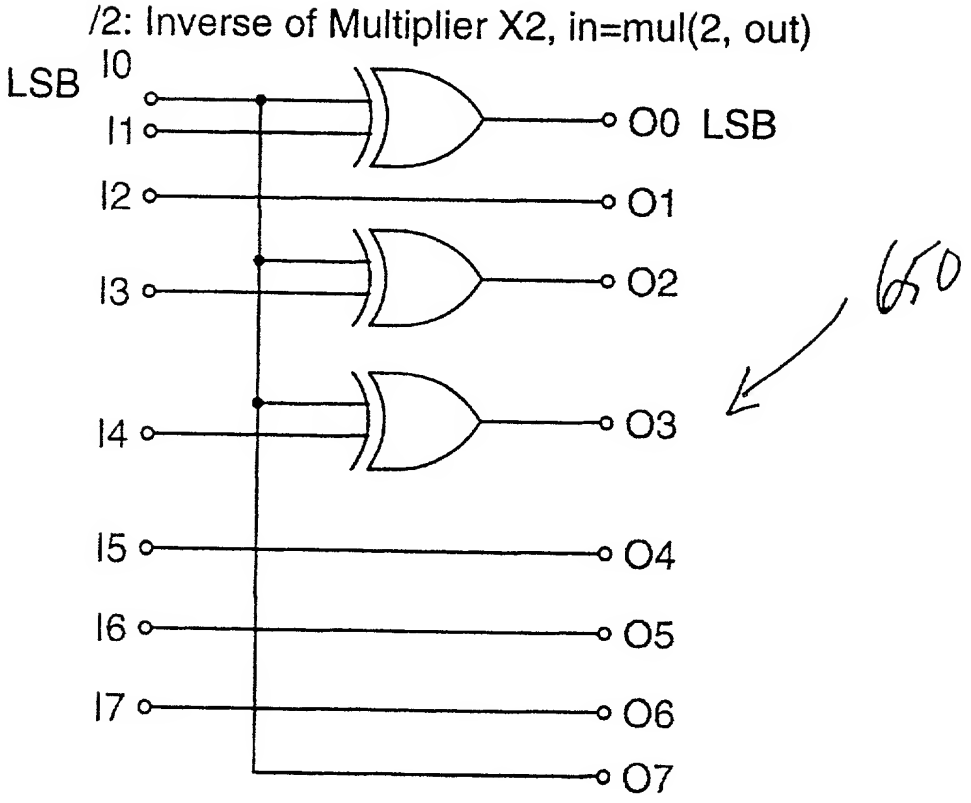

/2: Inverse of Multiplier X2, in=mul(2, out)
LSB
I0
I1
I2
I3
I4
I5
I6
I7
O0 LSB
O1
O2
O3
O4
O5
O6
O7
650

Figure 21

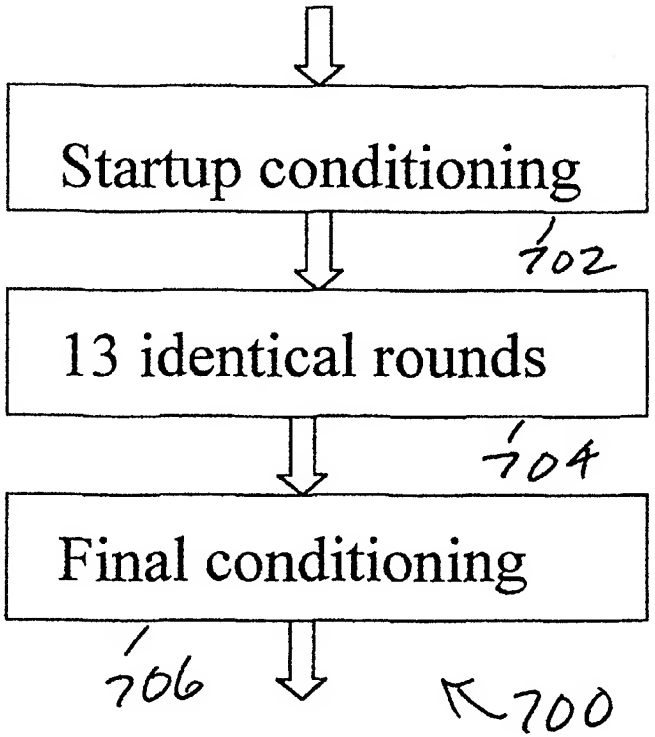

Startup conditioning
13 identical rounds
Final conditioning
702
704
706
700

Fig. 22

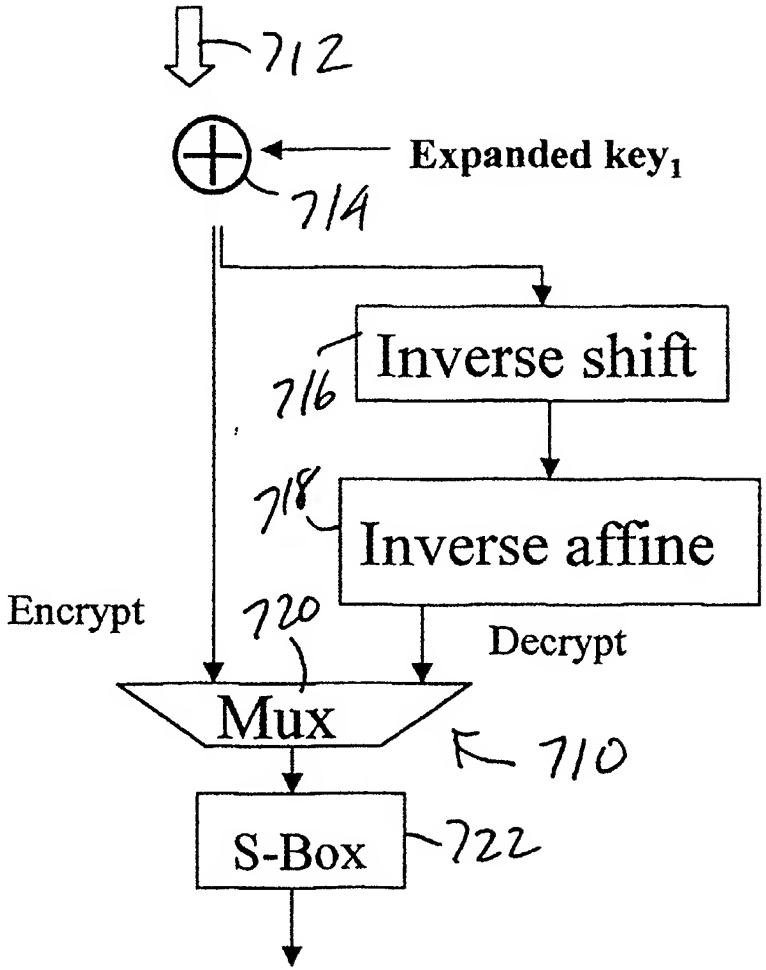

712
Expanded key1
714
Inverse shift
716
Inverse affine
718
Encrypt
720
Decrypt
Mux
710
S-Box
722

Fig. 23

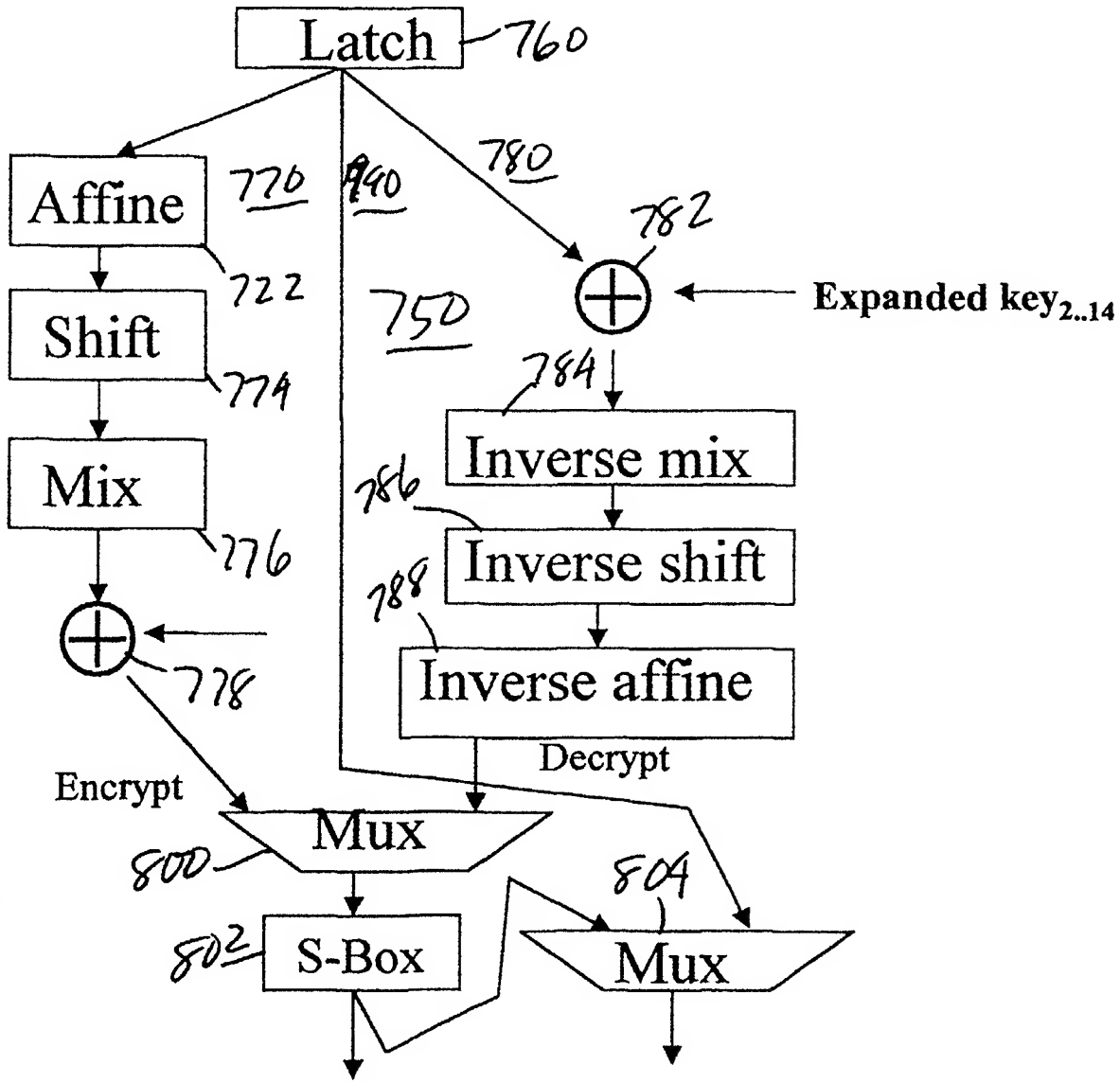

Latch
760
Affine
770
940
780
782
722
750
Shift
774
Expanded key2..14
784
Inverse mix
Mix
786
776
Inverse shift
788
778
Inverse affine
Decrypt
Encrypt
Mux
800
804
802
S-Box
Mux

Fig. 24

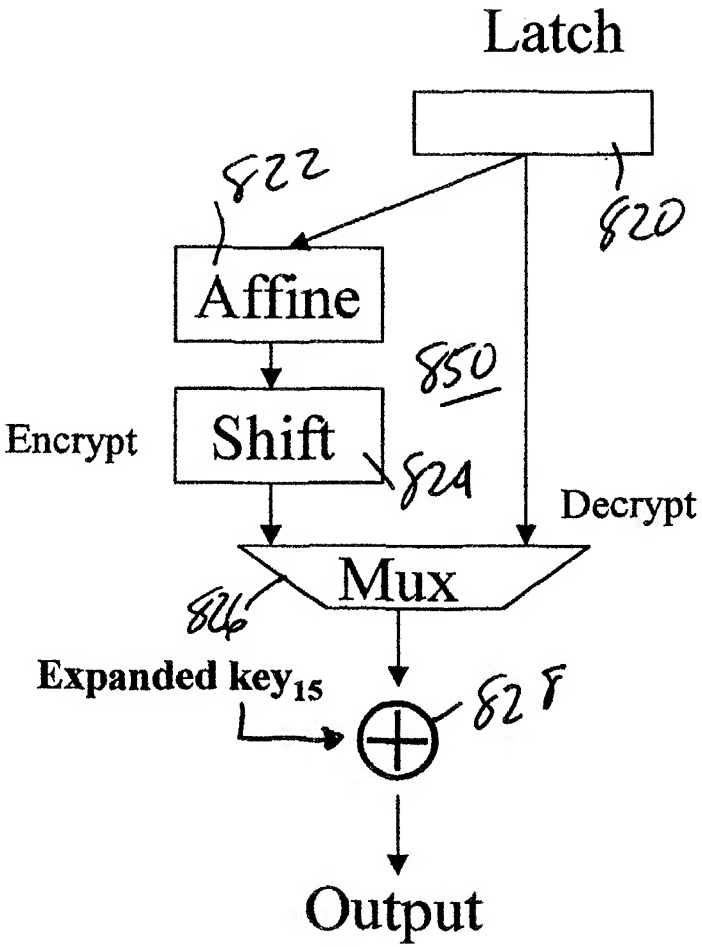

Latch
822
820
Affine
850
Encrypt
Shift
824
Decrypt
Mux
826
Expanded key15
828
Output

Fig. 25

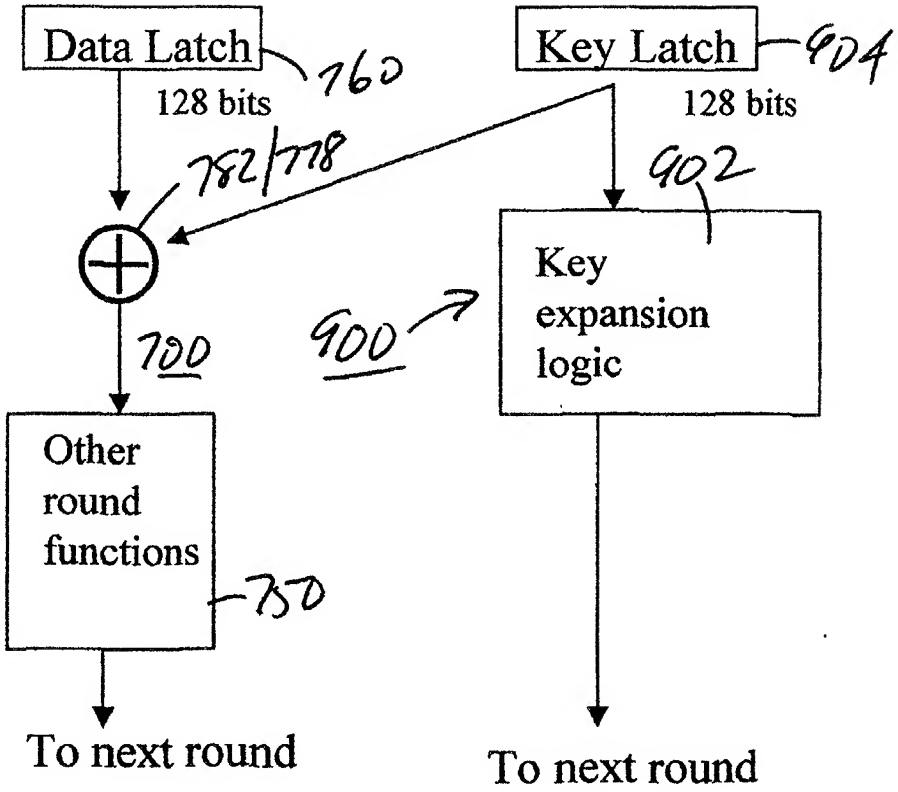

Data Latch
760
128 bits
Key Latch
904
128 bits
782/778
902
700
900
Key expansion logic
Other round functions
750
To next round
To next round

Fig. 26

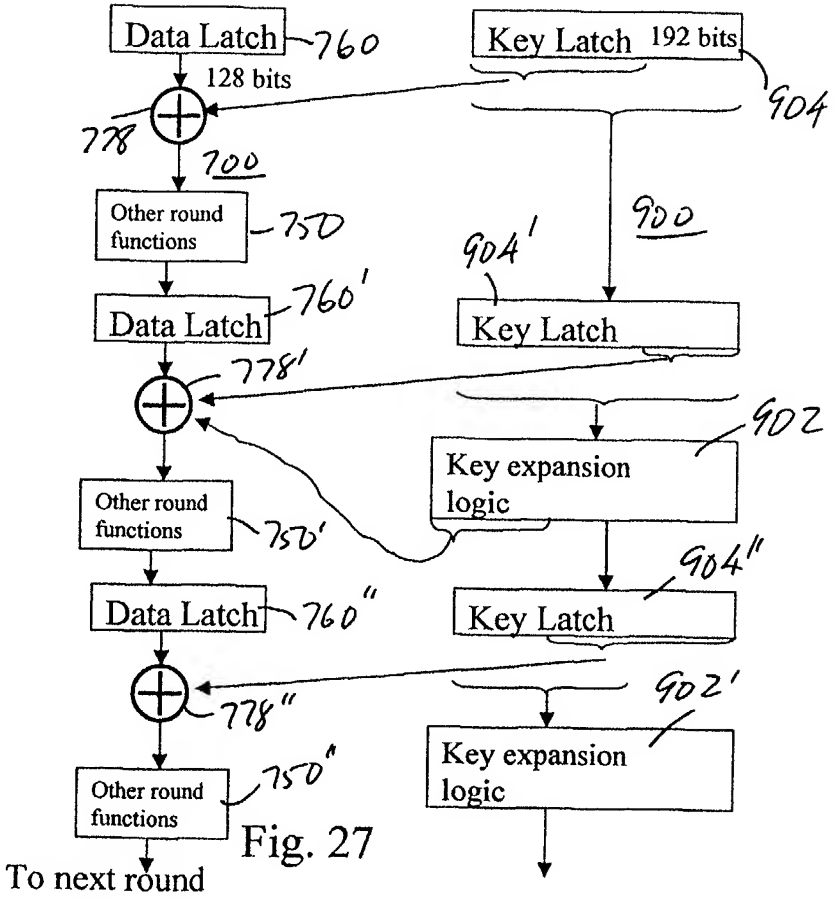


Fig. 27

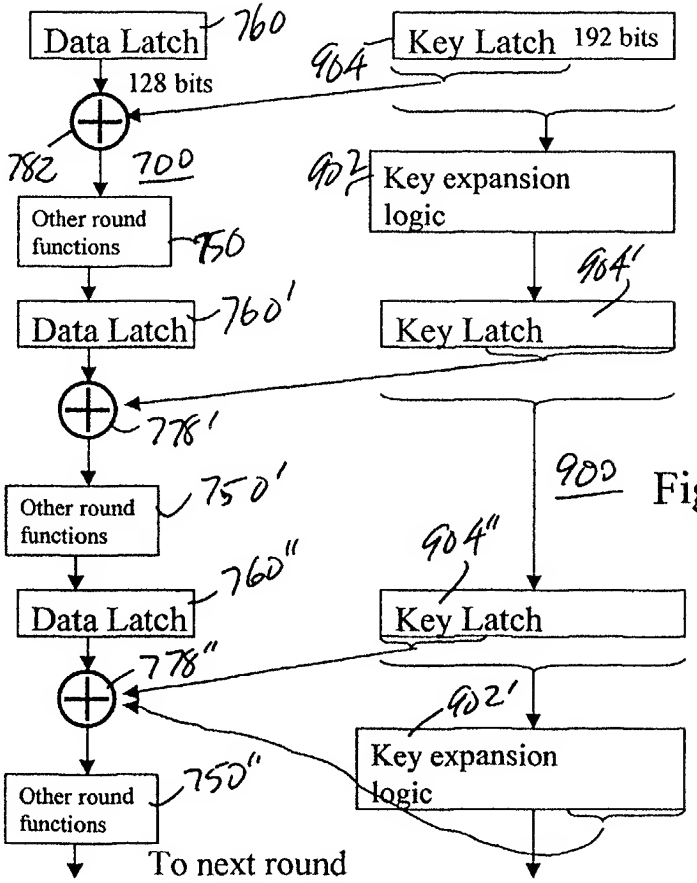

Data Latch
760
128 bits
782
700
Other round functions
750
Data Latch
760'
778'
Other round functions
750'
Data Latch
760"
778"
Other round functions
750"
To next round
Key Latch
192 bits
904
902
Key expansion logic
904'
Key Latch
900
904"
Key Latch
902'
Key expansion logic

Fig. 28

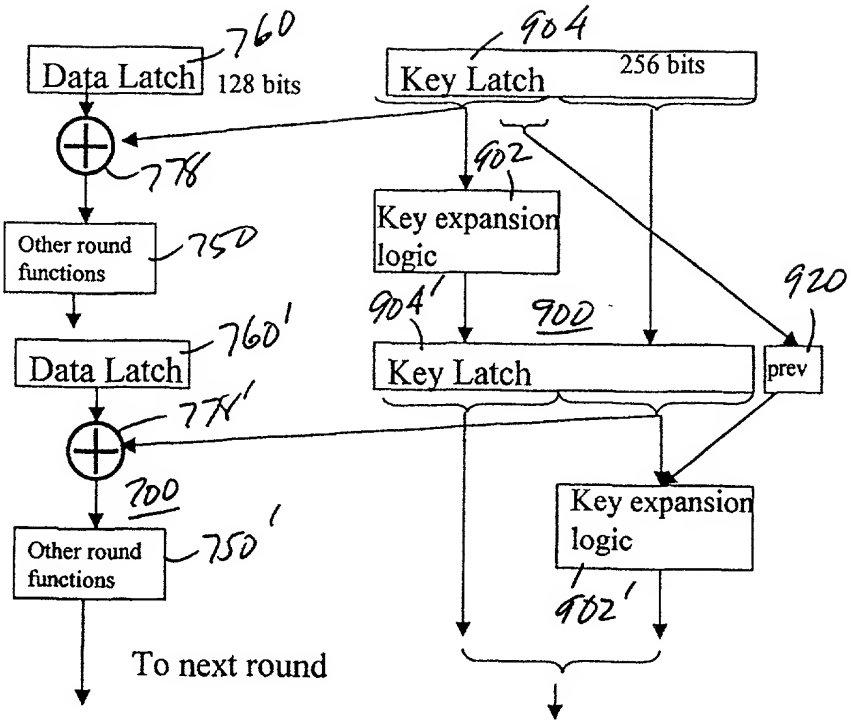

760
Data Latch
128 bits
904
Key Latch
256 bits
778
902
Key expansion logic
Other round functions
750
904'
900
920
760'
Data Latch
Key Latch
prev
774'
700
Key expansion logic
Other round functions
750'
902'
To next round

Fig. 29

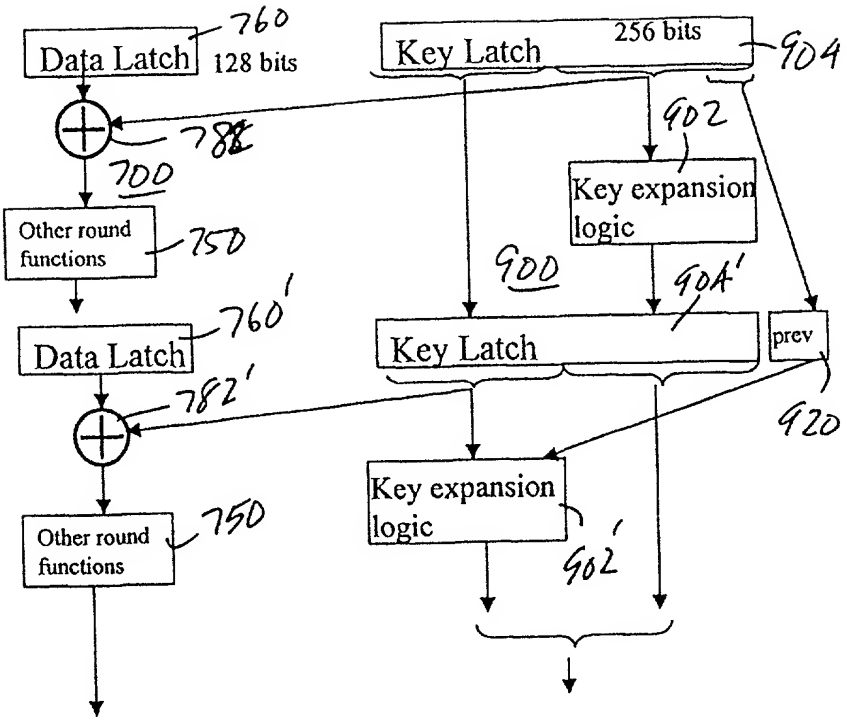

Data Latch
760
128 bits
Key Latch
256 bits
904
902
Key expansion logic
700
Other round functions
750
900
904'
Data Latch
760'
Key Latch
prev
782'
920
Key expansion logic
902'
Other round functions
750
To next round

Fig. 30

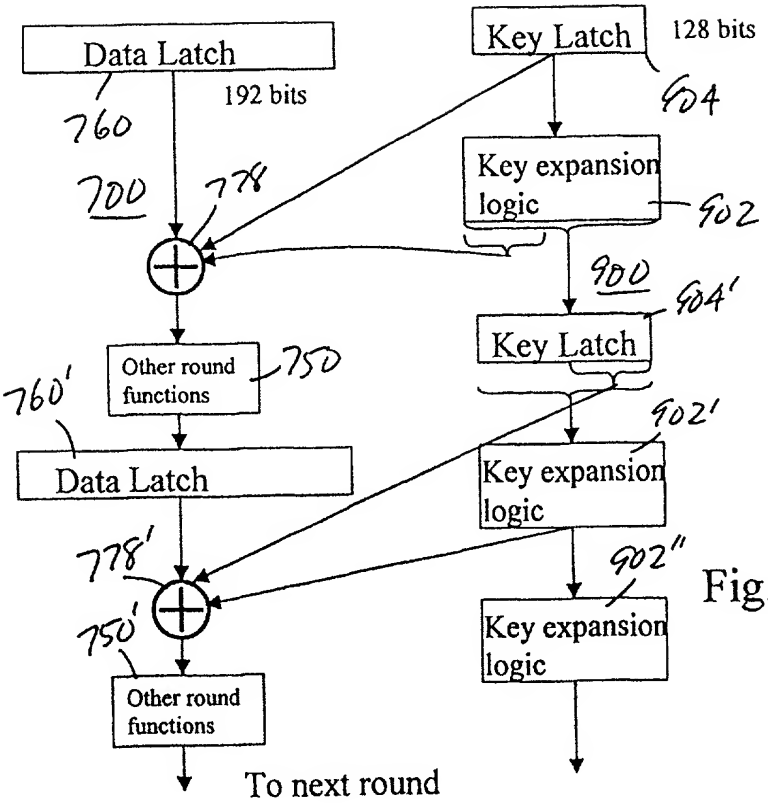

Data Latch
192 bits
760
700
778
Key Latch
128 bits
904
Key expansion logic
902
900
904'
Key Latch
Other round functions
750
760'
Data Latch
902'
Key expansion logic
778'
902"
750'
Key expansion logic
Other round functions
To next round

Fig. 31

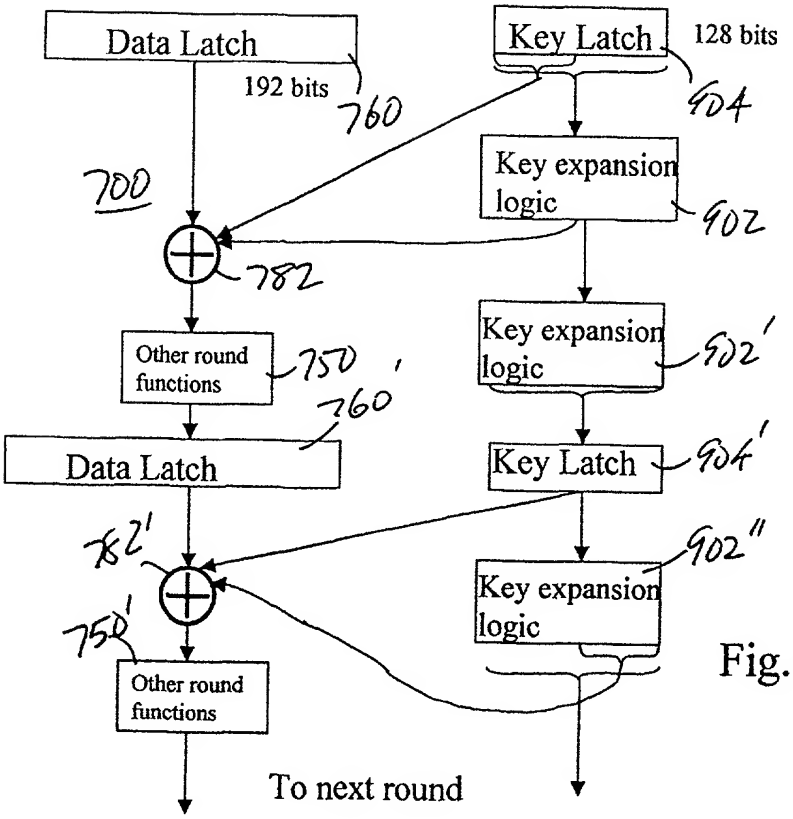

Data Latch
192 bits
760
Key Latch
128 bits
904
700
Key expansion logic
902
782
Other round functions
750
760'
Key expansion logic
902'
Data Latch
Key Latch
904'
782'
902"
Key expansion logic
750'
Other round functions
To next round

Fig. 32

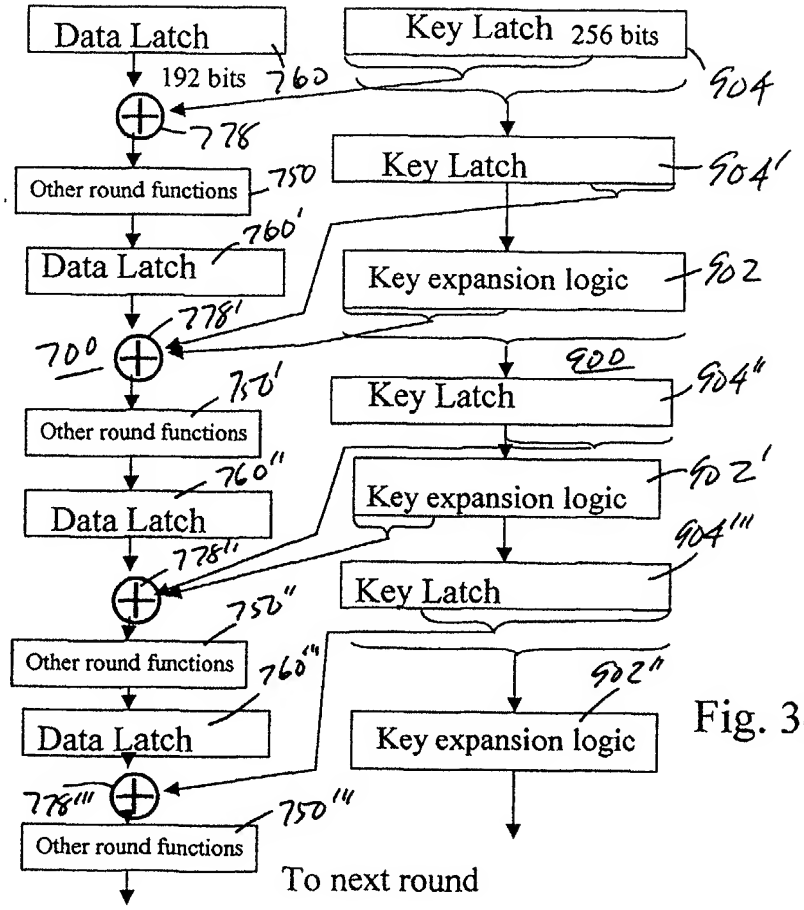

Data Latch
192 bits
760
Key Latch 256 bits
904
778
Other round functions
750
Key Latch
904'
760'
Data Latch
Key expansion logic
902
778'
700
900
Key Latch
904"
750'
Other round functions
760"
Data Latch
Key expansion logic
902'
778"
904"'
Key Latch
750"
Other round functions
760"'
902"
Data Latch
Key expansion logic
778"'
750"'
Other round functions
To next round

Fig. 34

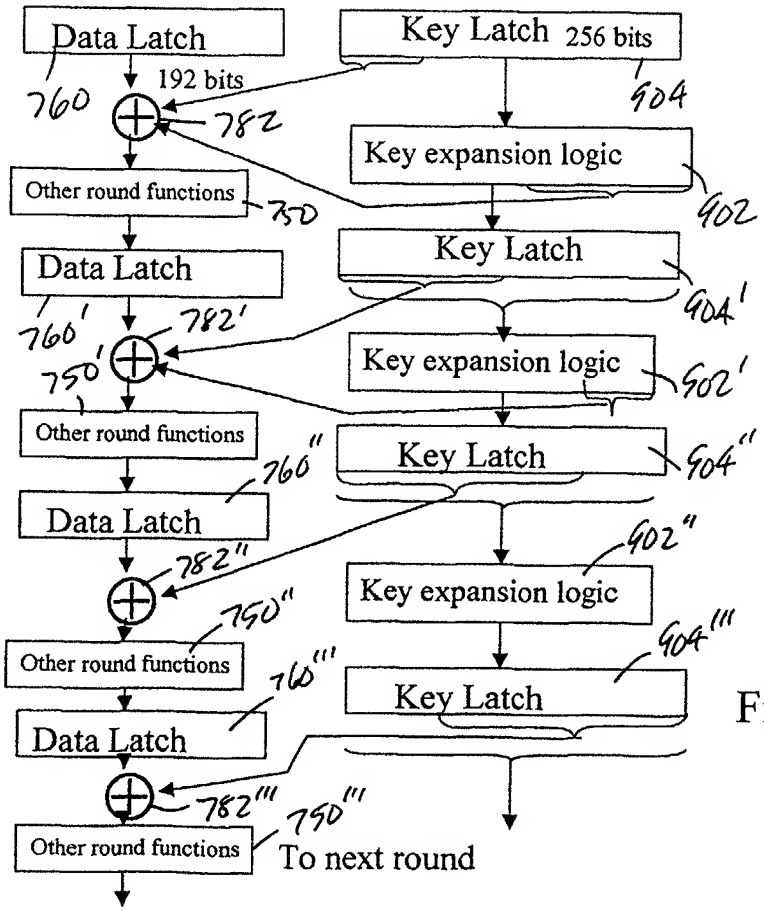

Data Latch
192 bits
760
782
Key Latch 256 bits
904
Key expansion logic
902
Other round functions
750
Data Latch
760'
782'
750'
Key Latch
904'
Key expansion logic
902'
Other round functions
Data Latch
760"
782"
750"
Key Latch
904"
Key expansion logic
902"
Other round functions
Data Latch
760'''
782'''
750'''
Key Latch
904'''
Other round functions
To next round

Fig. 35

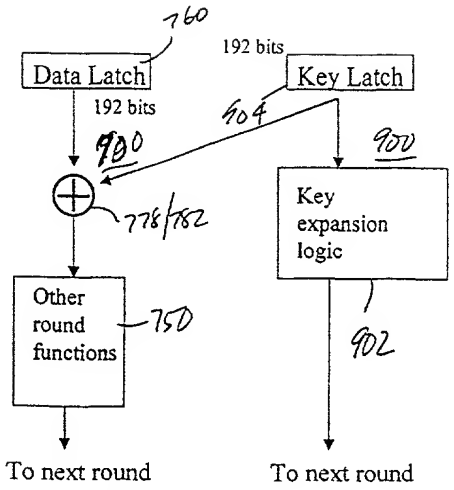

760
Data Latch
192 bits
192 bits
Key Latch
904
900
700
778/782
Other round functions
750
Key expansion logic
902
To next round
To next round

Fig. 33

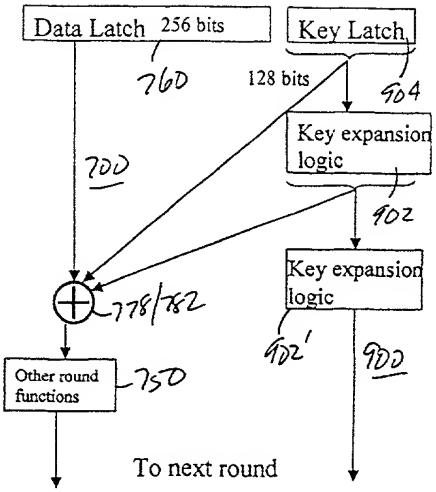

Data Latch
256 bits
760
Key Latch
128 bits
904
Key expansion logic
902
700
778/782
Key expansion logic
902'
900
Other round functions
750
To next round

Fig. 36

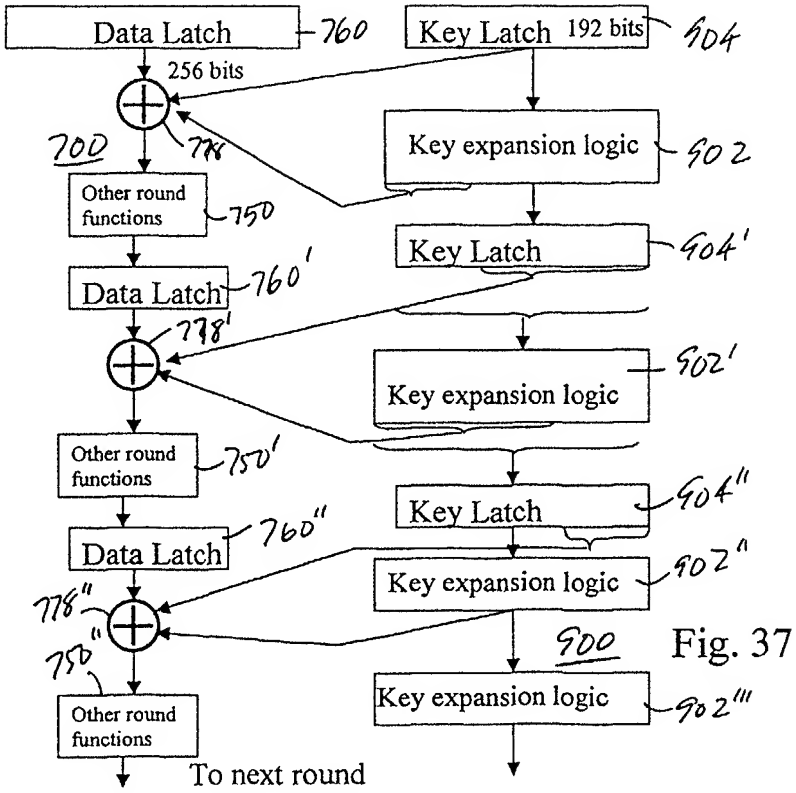

Data Latch
760
Key Latch 192 bits
904
256 bits
700
778
Key expansion logic
902
Other round functions
750
Key Latch
904'
Data Latch
760'
778'
Key expansion logic
902'
Other round functions
750'
Key Latch
904"
Data Latch
760"
Key expansion logic
902"
778"
750"
900
Key expansion logic
902'''
Other round functions
To next round

Fig. 37

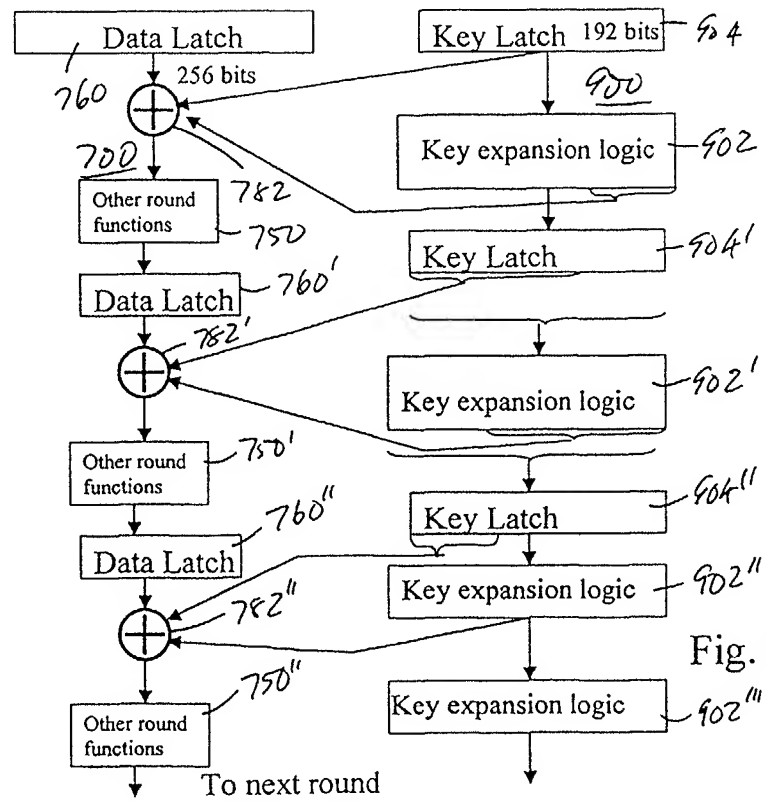

Data Latch
256 bits
Key Latch 192 bits
904
900
Key expansion logic
902
760
700
782
Other round functions
750
Key Latch
904'
Data Latch
760'
782'
Key expansion logic
902'
Other round functions
750'
Key Latch
904''
Data Latch
760''
Key expansion logic
902''
782''
750''
Other round functions
Key expansion logic
902'''
To next round

Fig. 38

Key expansion Logic

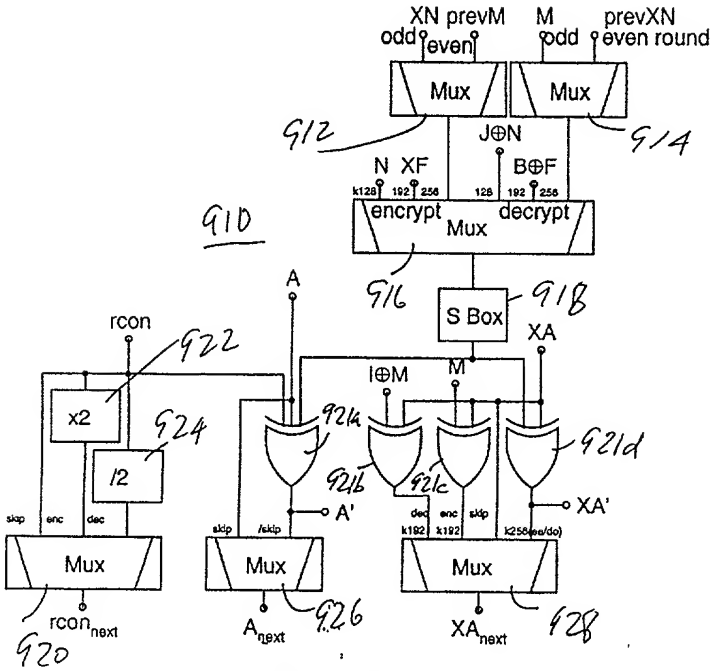
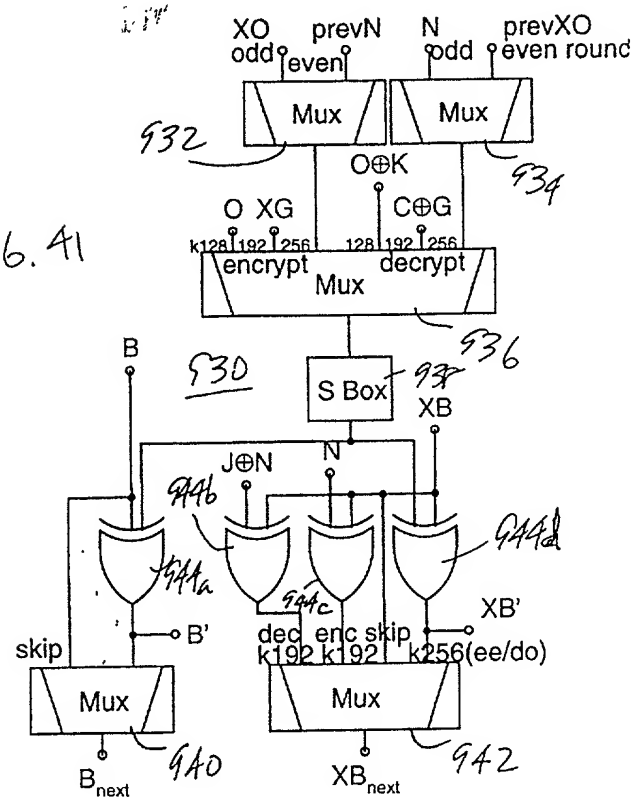


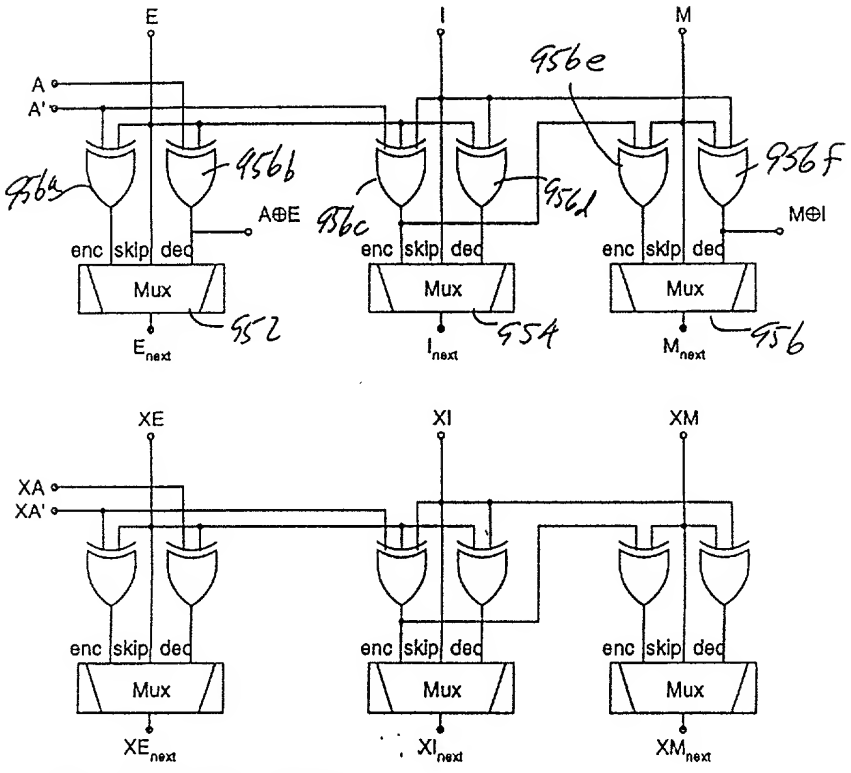
FIG. 4D

Key expansion Logic



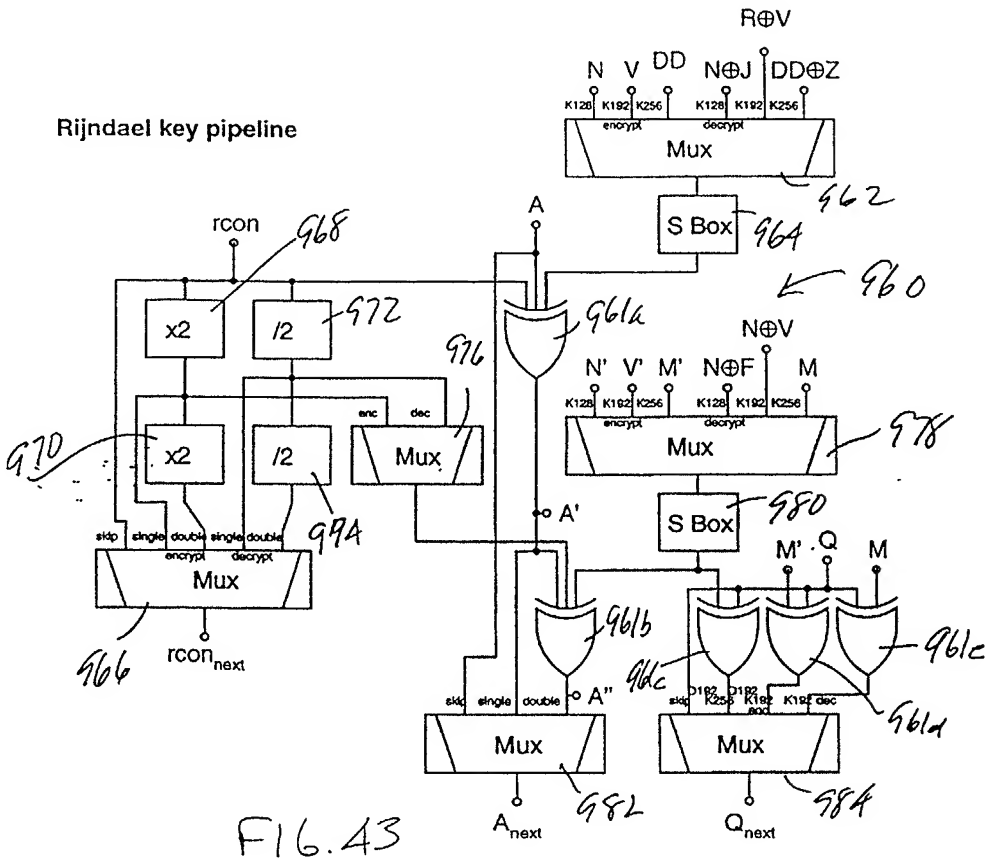
F16.41

950

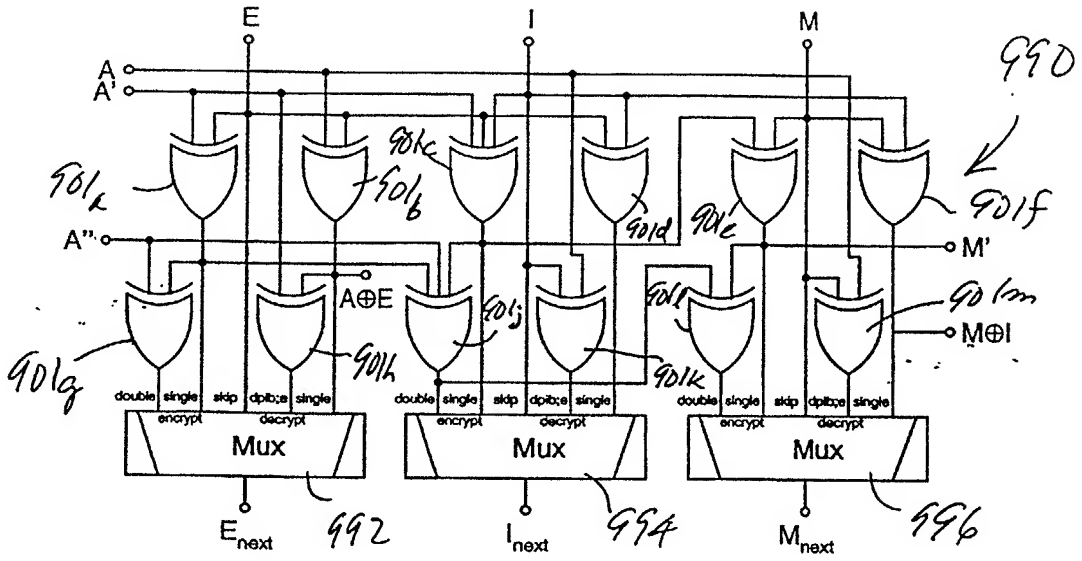


Key expansion Logic AES

FIG. 42


Rijndael key pipeline
R⊕V
N V DD N⊕J DD⊕Z
K128 K192 K256 K128 K192 K256
encrypt decrypt
Mux
962
S Box
964
960
A
rcon
968
x2
12
972
961a
N⊕V
N' V' M' N⊕F M
976
enc dec
Mux
978
970
x2
12
S Box
980
A'
994
skip single double single double
encrypt decrypt
Mux
966
rcon next
M' Q M
961b
961c
961d
A"
skip single double
Mux
Mux
982
984
A next
Q next

F16.43



Rijndael Key Pipeline

FIG. 44

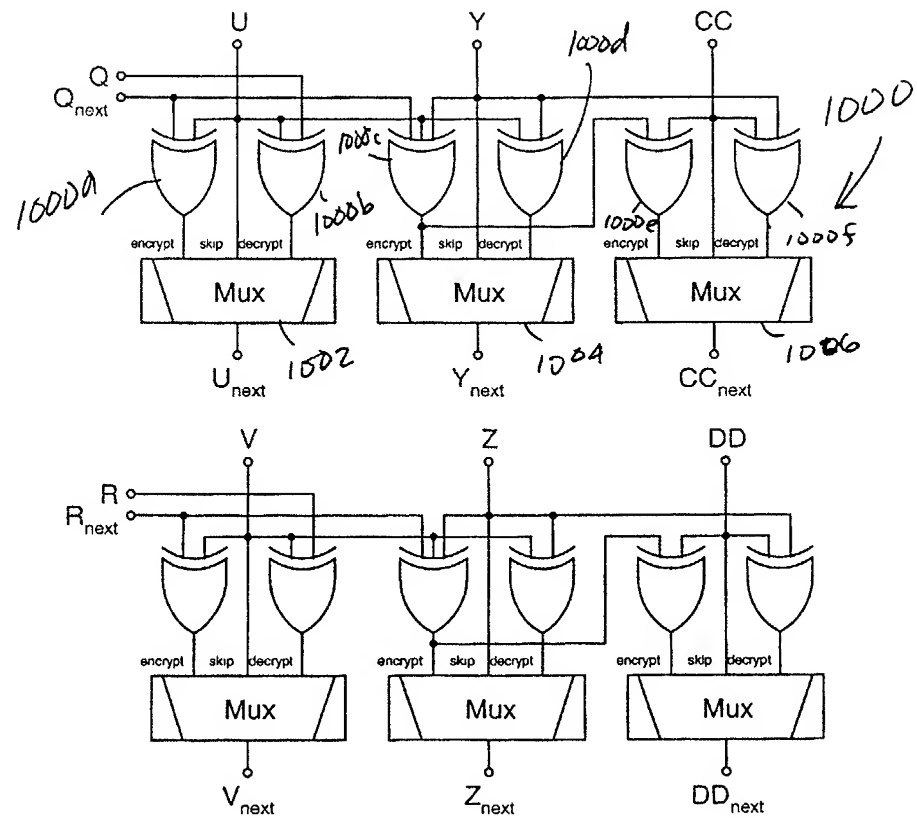


FIG. 45 **Rijndael Key Pipeline**